under the launch operator's control that contains an exposed site. An exposed site is any structure that may be occupied by human beings, and that has at least one window, excluding automobiles, airplanes, and waterborne vessels. A ''single residence,'' as used in section 6.3.2.4 of ANSI S2.20–1983 shall be treated as an exposed site. A launch operator shall use the most recent census information on each population center evaluated.

(ii) A launch operator shall determine the distance from the maximum credible impact explosion site to each population center potentially exposed. Unless the launch operator demonstrates, through the licensing process, that the potential explosion site is positively limited to a defined region, the distance between the potential explosion site and a population center must be the minimum distance between any point within the region contained by the flight control lines and the nearest exposed site within the population center.

(iii) A launch operator shall assume that weather conditions are optimized for a distant focus overpressure hazard and use an atmospheric blast focus factor (F) of 5 as defined by ANSI S2.20–1983.

(iv) For the purposes of this analysis, a population center shall be deemed vulnerable to the distant focus overpressure hazard if the ''no damage yield limit,'' calculated for the population center using the methodology in section 6.3.2.4 of ANSI S2.20–1983, is less than the maximum credible explosive yield. If there are no exposed sites that have a ''no damage yield limit'' that is less than the maximum credible explosive yield, the launch is exempt from any further requirements in this section.

(4) *Estimate the quantity of broken windows.* A launch operator shall use a focus factor of 5 and the methods provided by ANSI S2.20–1983 to estimate the number of potential broken windows within each population center determined to be vulnerable to the distant focus overpressure hazard in accordance with paragraph (b)(3) of this section.

(5) *Determine and implement measures necessary to prevent distant focus overpressure from breaking windows.* For each population center deemed vulnerable to a distant focus overpressure hazard, a launch operator shall determine and implement mitigation measures to protect the public from serious injury from broken windows. This may be accomplished by using one or more of the following measures:

(i) Apply 4-millimeter thick anti-shatter film to windows at all exposed sites.

(ii) Evacuate the exposed public to a location that is not vulnerable to the distant focus overpressure hazard at least two hours prior to the planned flight time.

(iii) If less than 20 windows are predicted to break, as determined in accordance with paragraph (b)(4) of this section, advise the public of the potential for glass breakage.

(iv) Measure the speed of sound as a function of altitude for the time of flight and conduct launches only when an inversion in the sonic velocity profile does not exist within ±30 degrees azimuth toward any population center vulnerable to a distant focus overpressure hazard, accounting for uncertainty in the meteorological conditions present during flight. For a launch operator to use this approach as a mitigation measure, a launch operator shall demonstrate that no window breakage is predicted in any population center due to a maximum credible yield explosion using the analysis methods in section 6.3.2.4.1 of ANSI S2.20–1983. A launch operator may also refine its analysis by performing acoustic ray path calculations to determine the actual focusing region and the focusing factor (F) that apply to a launch as described in section 5.1.3 of ANSI S2.20–1983 using the referenced computer methods.

(c) *Probabilistic distance focusing overpressure analysis.* When mitigation measures cannot be used a launch operator may apply statistical risk management to control the distant focus overpressure hazard. When proposing to follow this approach, a launch operator shall demonstrate through a distant focus overpressure risk analysis that the launch will be conducted in accordance with the public risk criteria contained in § 417.107(b). The FAA will evaluate any distant focus overpressure risk analysis on a case-by-case basis.

(d) *Distant focus over pressure blast effect products.* The products of a launch operator's distant focus overpressure analysis to be submitted in accordance with § 417.203(c) must include the following:

(1) A launch operator shall submit a description of the methodology used to produce the distant focus overpressure analysis results, a tabular description of the analysis input data, and a description of any distant focus overpressure mitigation measures implemented. If the launch operator elects to measure the speed of sound as a function of altitude and conduct launches only when a focusing condition toward populated areas does not exist, the launch operator shall submit a description of the method for evaluating weather parameters to determine the existence of conditions that will permit the launch operator to comply with the distant focus overpressure requirements of this section.

(2) A launch operator shall submit one example set of any distant focus overpressure risk analysis computations.

(3) A launch operator shall submit the values for the maximum credible explosive yield as a function of time of flight.

(4) A launch operator shall identify the distance between the potential explosion site and any population center vulnerable to the distant focus overpressure hazard. For each population center, the launch operator shall identify the exposed populations by location and number of people.

(5) A launch operator shall describe any mitigation measures established to protect the public from distant focus overpressure hazards and any flight commit criteria established to ensure the mitigation measures are enforced.

§ 417.233 Conjunction on launch assessment.

(a) *General.* A licensee shall obtain a conjunction on launch assessment performed by United States Space Command. A licensee shall implement any launch waits in a planned launch window identified by the conjunction on launch assessment during which flight must not be initiated, in order to maintain a 200-kilometer separation from any inhabitable orbiting object in accordance with § 417.107. A licensee may request a conjunction on launch assessment be performed for other orbital objects to meet mission needs or to accommodate other satellite owners or operators.

(b) *Conjunction on launch assessment analysis constraints.* A launch operator shall satisfy the following when obtaining and implementing the results of a conjunction on launch assessment:

(1) A licensee shall provide United States Space Command with the launch window and trajectory data needed to perform a conjunction on launch assessment for a launch as required by paragraph (c) of this section, at least 15 days before the first attempt at flight. The FAA will identify a licensee to United States Space Command as part of issuing a license and provide a licensee with current United States Space Command contact information.

(2) A licensee shall obtain a conjunction on launch assessment performed by United States Space

Command 6 hours before the beginning of a launch window.

(3) A conjunction on launch assessment is valid for 12 hours from the time that the state vectors of the inhabitable orbiting objects were determined. If an updated conjunction on launch assessment is needed due to a launch delay, a licensee shall submit the request at least 12 hours prior to the next launch attempt.

(4) For every 90 minutes, or portion of 90 minutes, that pass between the time United States Space Command last determined the state vectors of the orbiting objects, a licensee shall expand each launch window wait by subtracting 15 seconds from the start of the launch window wait and adding 15 seconds to the end of the launch window wait. A launch operator shall incorporate the resulting launch window waits into its flight commit criteria established in accordance with § 417.113.

(c) *Information required.* A launch operator shall prepare a conjunction on launch assessment worksheet for each launch using a standardized format that contains the input data required by this paragraph. An example conjunction on launch assessment worksheet is provided in figure 417.233–1. A launch operator licensee shall submit the input data to United States Space Command for the purposes of completing a conjunction on launch assessment. A launch operator license applicant shall submit the input data to the FAA as part of the license application process according to § 415.115 of this chapter.

(1) *Launch information.* A launch operator shall submit the following launch information:

(i) *Mission name.* A mnemonic given to the launch vehicle/payload combination identifying the launch mission from all others.

(ii) *Segment number.* A segment is defined as a launch vehicle stage or payload after the thrusting portion of its flight has ended. This includes the jettison or deployment of any stage or payload. A separate worksheet is required for each segment. For each segment, a launch operator shall determine the ''vector at injection'' as defined by paragraph (c)(5) of this section. Each segment number shall be provided as a sequence number relative to the total number of segments for a launch, such as ''1 of 5.''

(iii) *Launch window.* The launch window opening and closing times in Greenwich Mean Time (referred to as ZULU time on the sample form) and the Julian dates for each scheduled launch attempt.

(2) *Point of contact.* The person or office within a licensee's organization that collects, analyzes, and distributes conjunction on launch assessment results.

(3) *Conjunction on launch assessment analysis results transmission medium.* A launch operator shall identify the transmission medium, such as voice, FAX, or e-mail, for receiving results from United States Space Command.

(4) *Requestor launch operator needs.* A launch operator shall indicate which of the following analysis output formats it requires for establishing flight commit criteria for a launch:

(i) *Waits.* The times within the overall launch window during which flight must not be initiated.

(ii) *Windows.* The times within an overall launch window during which flight may be initiated.

(5) *Vector at injection.* A launch operator shall identify the vector at injection for each segment. The term ''vector at injection'' is used to identify the position and velocity vectors after the thrust for a segment has ended. The term was originally used to refer to a segment upon orbital injection, but in practice is used to describe any segment of a launch, whether orbital or suborbital.

(i) *Epoch.* The epoch time, in Greenwich Mean Time (GMT), of the expected launch vehicle liftoff time.

(ii) *Position and velocity.* The position coordinates in the EFG coordinate system in kilometers and the velocity coordinates in the coordinate system in kilometers per second, of each launch vehicle stage or payload after any burnout, jettison, or deployment.

(6) *Time of powered flight.* The elapsed time in seconds, from liftoff, for the launch vehicle to arrive at the vector at injection. For each stage or component jettisoned, the time of powered flight shall be measured from liftoff.

(7) *Time span for launch window file (LWF).* A launch operator shall provide the following information regarding its launch window:

(i) *Launch window.* The launch window measured in minutes from the initial proposed liftoff time.

(ii) *Time of powered flight.* The time given in paragraph (c)(6) of this section measured in minutes rounded up to the nearest integer minute.

(iii) *Screen duration.* The time duration, after all thrusting periods of flight have ended, that a conjunction on launch assessment must screen for potential conjunctions with orbital objects. Screen duration is measured in minutes and must be greater than or equal to 100 minutes for an orbital launch.

(iv) *Extra pad.* An additional period of time for conjunction on launch assessment screening to ensure the entire first orbit is evaluated. This time shall be 10 minutes unless otherwise specified by United States Space Command.

(v) *Total.* The summation total of the time spans provided in paragraphs (c)(7)(i) through (c)(7)(iv) of this section expressed in minutes.

(8) *Screening.* A launch operator shall select spherical or ellipsoidal screening as defined in this paragraph for determining any conjunction. The default shall be the spherical screening method using an avoidance radius of 200 kilometers for habitable orbiting objects. If the launch operator requests screening for any uninhabitable objects, the default shall be the spherical screening method using a miss-distance of 25 kilometers.

(i) *Spherical screening.* Spherical screening utilizes an impact exclusion sphere centered on each orbiting object's center-of-mass to determine any conjunction. A launch operator shall specify the avoidance radius for habitable objects and for any uninhabitable objects if the launch operator elects to perform the analysis for uninhabitable objects.

(ii) *Ellipsoidal screening.* Ellipsoidal screening utilizes an impact exclusion ellipsoid of revolution centered on the orbiting object's center-of-mass to determine any conjunction. A launch operator shall provide input in the UVW coordinate system in kilometers. The launch operator shall provide delta-U measured in the radial-track direction, delta-V measured in the in-track direction, and delta-W measured in the cross-track direction.

(9) *Orbiting objects to evaluate.* A launch operator shall identify the orbiting objects to be included in the analysis.

(10) *Deliverable schedule/need dates.* A launch operator shall identify the times before flight, ''L-times,'' that the conjunction on launch assessment is needed.

(d) *Conjunction on launch assessment products.* A launch operator must submit its conjunction on launch assessment products according to § 417.203(c) and must include the input data required by paragraph (c) of this section. A launch operator licensee shall incorporate the result of the conjunction on launch assessment into its flight commit criteria established in accordance with § 417.113.

Figure 417.233-1, Example Conjunction On Launch Assessment Worksheet.

Pre-Launch Conjunction On Launch Assessment Worksheet			
Launch Information		**Point of Contact**	
Name:		Voice DSN:	
Segment Number:	of	Voice Comm:	
Launch Window		FAX DSN:	
Julian Date:		FAX Comm:	
Open Time:		CFL:	
Close Time:		E-mail	

Requestor Needs (circle choices)		Send Results via (circle choices)		
Waits	Windows	E-mail	FAX	Voice

Vector at Injection		Time of Powered Flight (ToPF)	
E (km):			seconds
F (km):		Time Span For LWF (minutes)	
G (km):		Launch Window:	
ED (km/s):		ToPF:	
FD (km/s):		Screen Duration:	
GD (km/s):		Extra Pad:	10
Epoch (s):		Total:	

Spherical Screening (Y/N) Avoidance Radius (km)		Ellipsoidal Screening (Y/N) Delta (km)	
Uninhabitable Objects:		Radial-Track (ΔU):	
		In-Track (ΔV):	
Inhabitable Objects:		Cross-Track (ΔW):	

Orbiting Objects to Evaluate (circle choice)		
Inhabitable Only	All Objects	Inhabitable and Other: (specify)

Runs Due			
L-	L-	L-	L-
L-	L-	L-	L-
L-	L-	L-	L-

§ 417.235 Analysis for launch of an unguided suborbital rocket flown with a wind weighting safety system.

(a) *General.* The requirements of this section apply to the launch of an unguided suborbital rocket. A launch operator shall perform a flight safety analysis to determine the launch parameters and conditions under which an unguided suborbital rocket may be flown using a wind weighting safety system. The results of this analysis must demonstrate that any adverse effects resulting from flight will be contained within controlled operational areas and any flight hardware or payload impacts will occur within planned impact areas. The flight safety analysis must demonstrate compliance with the safety criteria and operational requirements of § 417.125 and must include the other analyses required by this section. The flight safety analysis must be conducted in accordance with appendixes B and C of this part.

(b) *Trajectory analysis.* A launch operator shall perform a trajectory analysis to determine an unguided suborbital rocket's nominal trajectory and three-sigma dispersed trajectories using the methods provided in appendix C of this part.

(c) *Hazard area analysis.* A launch operator shall perform a hazard area analysis to determine the land, sea, and air areas that must be monitored, controlled, or evacuated in order to protect the public from the adverse effects of planned unguided suborbital rocket flight events. A flight hazard area, impact hazard area, ship hazard area, and aircraft hazard area must be determined using the methods required by appendix C.

(d) *Debris risk analysis.* A launch operator shall perform a risk analysis to determine public risk for the expected average number of casualties (E_C) due to potential inert and explosive debris impacts resulting from planned or unplanned events occurring during the flight of an unguided suborbital rocket. The analysis shall account for the risk to all populations on land. A debris risk analysis must account for unguided suborbital rocket failure probability, flight dwell times over populated or other protected land areas, five-sigma lateral trajectory dispersion for a normal unguided suborbital rocket, effective casualty area of impacting debris, and population densities. The results of a launch operator's debris risk analysis must demonstrate that the launch will be conducted in accordance with the public risk criteria contained in § 417.107(b). A launch operator shall perform a debris risk analysis for the launch of an unguided suborbital rocket in accordance with § 417.227 and using the methodology provided in appendix B of this part.

(e) *Wind weighting analysis.* A launch operator shall perform a wind weighting analysis to determine launcher azimuth and elevation settings that correct for the windcocking and wind-drift effects on an unguided suborbital rocket due to wind forces. A launch operator shall perform a wind weighting analysis using the method provided in appendix C of this part and in accordance with the following:

(1) A wind weighting analysis must ensure that three-sigma of all wind weighted stage or other component impacts are contained within a three-sigma performance impact dispersion ellipse about the nominal no-wind impact point, assuming a normal bivariate Gaussian distribution. When determining stage (or impacting body) wind weighted impact points, a launch operator shall account for three standard deviation variations in ballistic performance error parameters, including wind measurement errors and errors in modeled response to wind forces.

(2) A launch operator shall perform an initial wind weighting analysis prior to flight to predict the effects of forecasted or statistical winds on impact point displacement during thrusting phases of flight as well as ballistic free-fall of each unguided suborbital rocket stage until impact.

(3) A launch operator shall perform a final wind weighting analysis as part of the launch-day countdown process with actual measured wind data.

(4) A launch operator shall use the results of a wind weighting analysis and the wind conditions for which the analysis is valid as the basis for flight commit criteria developed in accordance with § 417.113.

(f) *Conjunction on launch assessment.* A launch operator shall ensure that a conjunction on launch assessment is performed for the flight of an unguided suborbital rocket in accordance with § 417.233.

(g) *Products.* The products of a launch operator's flight safety analysis for launch of an unguided suborbital rocket to be submitted in accordance with § 417.203(c) must include the trajectory analysis products, hazard area analysis products, and wind weighting analysis products required by appendix C of this part. A launch operator shall also submit debris risk analysis products in accordance with § 417.227 and conjunction on launch assessment products in accordance with § 417.233.

§§ 417.236–417.300 [Reserved]

Subpart D—Flight Safety System

§ 417.301 General.

(a) A launch operator shall use a flight safety system that provides a means of preventing a launch vehicle and its hazards, including any payload hazards, from reaching the public in the event of a launch vehicle failure during flight. Requirements that define when a launch operator must employ a flight safety system are provided in § 417.107(a).

(b) A flight safety system must consist of a flight termination system, a command control system, and the support systems defined in this subpart, including all associated hardware and software unless the requirements of § 417.107(a)(3) apply. A flight safety system also includes the functions of any personnel who operate flight safety system hardware and software. A launch operator shall satisfy each requirement of this subpart, including all requirements contained in referenced appendices, by meeting the requirements or by using an alternate method approved by the FAA through the licensing process. If a flight safety system does not satisfy all the requirements of this subpart, the requirements of § 417.107(a)(3) apply. The FAA will approve an alternate method if a launch operator provides a clear and convincing demonstration that its proposed method provides an equivalent level of safety to that required by this subpart. A launch operator shall obtain FAA approval of any proposed alternate method before its license application or application for license modification will be found sufficiently complete to initiate review pursuant to § 413.11 of this chapter.

(c) A launch operator's test program, required by § 417.115, must demonstrate the ability of a flight safety system to meet the design margins and reliability requirements of this subpart and the ability of the flight safety system to function without degradation in performance when subjected to non-operating and operating environments. The test program must satisfy the requirements of § 417.115 and include tests of the flight termination system and command control system as required by §§ 417.315, 417.317 and 417.325. The test program must include tests of the support systems required by § 417.327 and the equipment and instrumentation associated with the flight safety system, including real-time computers, display systems, consoles, telemetry, command control, tracking systems, and video systems. The cause of any test failure must be determined, corrective actions implemented, and additional testing performed to demonstrate that the test criteria are satisfied before flight.

(d) Any change to a licensee's flight safety system design or flight safety system test program that was not coordinated during the licensing process must be submitted to the FAA for approval as a license modification prior to flight.

(e) Prior to the flight of each launch vehicle, a licensee shall confirm to the FAA in writing that its flight safety system is as described in its license application, including all applicable application amendments and license modifications, and complies with all terms of the license and the requirements of this part.

(f) Upon review of a proposed launch, the FAA may identify and impose additional requirements needed to address unique issues presented by a flight safety system, including its design, operational environments, and testing.

§ 417.303 Launch vehicle flight termination system functional requirements.

(a) A launch operator shall use a flight termination system as part of a flight safety system. A flight termination system consists of all hardware and software onboard a launch vehicle needed to accomplish all flight termination functions in accordance with this section.

(b) Once initiated, a flight termination system must render each stage and any other propulsion system, including any propulsion system that is part of a payload that has the capability of reaching a populated or other protected area, non-propulsive, without significant lateral or longitudinal deviation in the impact point. A flight termination system must terminate flight in each thrusting stage and propulsion system. Any stage or propulsion system not thrusting at the time the flight termination system is initiated must be rendered incapable of becoming propulsive.

(c) The flight termination of one stage must not sever interconnecting flight termination system circuitry or ordnance of another stage until the flight termination of the other stage has been initiated.

(d) A flight termination system must destroy the pressure integrity of all solid propellant stages and strap-on motors. A flight termination system must terminate all thrust, or any residual thrust must cause a solid propellant stage or strap-on motor to tumble without significant lateral or longitudinal deviation in the impact point.

(e) A flight termination system must cause dispersion of any liquid propellant, whether by rupturing the propellant tank or other equivalent method, and initiate burning of any toxic liquid propellant.

(f) A flight termination system must not detonate any solid or liquid propellant.

(g) A flight termination system must include a command destruct system that is initiated by radio command and implemented in accordance with § 417.309. The FAA will approve another method, such as an autonomous flight termination system, if a launch operator provides a clear and convincing demonstration, through the licensing process, that its proposed method provides an equivalent level of safety.

(h) A flight termination system must provide for flight termination of any inadvertently or prematurely separated stage or strap-on motor capable of reaching a populated or other protected area before orbital insertion. Each stage or strap-on motor that does not possess its own complete command destruct system in accordance with § 417.309 must be equipped with an inadvertent separation destruct system that complies with the requirements of § 417.311.

§ 417.305 Flight termination system reliability.

(a) *Reliability design.* A flight termination system must have a reliability design of 0.999 at a confidence level of 95 percent. A launch operator shall conduct system reliability analyses according to § 417.329 to demonstrate whether a flight termination system has the required reliability design.

(b) *Single fault tolerant.* A flight termination system, including monitoring and checkout circuits, must not have a single failure point that would inhibit functioning of the system or produce an inadvertent output. Exceptions to this requirement apply to certain components that are identified in this subpart and that meet the design and test requirements in appendixes D and E of this part.

(c) *Redundancy.* A flight termination system must utilize redundant component strings in accordance with the following:

(1) Redundant components shall be structurally, electrically, and mechanically separated and mounted in different orientations on different axes.

(2) A flight termination system need not use redundant linear shaped charges, if, when employing a single linear shaped charge, the charge initiates at both ends, and the initiation source for one end is independent of the initiation source used for the other end.

(3) Passive components such as antennas and radio frequency couplers are not required to be physically redundant if they satisfy the requirements of appendix D of this part.

(d) *System independence.* A flight termination system must not share any power sources, cabling, or any other component with any other launch vehicle system. With the exception of any telemetry monitor signal and any engine shut-down output signal, a flight termination system must operate independently of all other vehicle systems.

(e) *Components and parts.* A licensee is responsible for the overall design of a flight termination system and shall ensure that all flight termination system components satisfy the requirements of appendix D of this part and all electronic piece parts used in a flight termination system component satisfy the requirements of appendix F of this part. A launch operator shall ensure that each flight termination system component and electronic piece part has written performance specifications that contain the particulars of how the component or piece part satisfies the requirements of appendixes D and F as related to the specific design of the flight termination system that contains the component or piece part.

(f) *Testability.* The design of a flight termination system and associated ground support and monitoring equipment shall provide for preflight testing performed in accordance with § 417.317.

(g) *Software and firmware.* A launch operator shall ensure that each software safety critical function associated with a flight termination system is identified, and that all associated computing systems, software, or firmware is designed, compiled, analyzed, tested, and implemented in accordance with § 417.123 and appendix H of this part. The requirements of appendix H also apply to any computing system, software, or firmware that must operate properly to ensure that the flight safety official has the accurate vehicle performance data needed to make a flight termination decision.

(h) *Component storage, operating, and service life.* All flight termination system components must have a specified storage life, operating life, and service life. Service life is the total time that a component spends in storage and after installation on the launch vehicle through the end of flight. The storage or service life of a component must start upon completion of the component's acceptance testing. Operating life must start upon activation of the component or installation of the component on a launch vehicle, whichever is earlier. A flight termination system component must function without degradation in performance when subjected to the full length of its specified storage life, operating life, and service life. A launch operator shall ensure that each component used in a flight termination system does not exceed its storage, operating, or service life before flight. A launch operator shall ensure that age surveillance testing, in accordance with appendix E of this part, is performed to verify or extend a component's storage, operating, or service life.

§ 417.307 Flight termination system environment survivability.

(a) *General.* The design of a flight termination system and its components, including all mounting hardware, cables and wires, must provide for the system and each component to function without degradation in performance when subjected to dynamic environment levels greater than those that it will experience during environmental stress screening tests, ground transportation, storage, launch processing, system checkout, and flight up to the point that the launch vehicle could no longer impact any populated or other protected area, or when subjected to dynamic environment levels greater than those that would cause structural breakup of the launch vehicle.

(b) *Maximum predicted environments.* A launch operator shall determine, based on analysis, modeling, testing, or flight data, all maximum predicted environments for the non-operating and operating environments that a flight termination system is to experience. The non-operating and operating environments must include, but need not be limited to, thermal range, vibration, shock, acceleration, acoustic, and other environments where applicable to a launch, such as humidity, salt fog, dust, fungus, explosive atmosphere, and electromagnetic energy. The specific environments that apply to the design of flight termination system components are identified in appendix D of this part. A launch operator shall determine each maximum predicted environment in accordance with the following:

(1) If there are fewer than three samples of flight data, a launch operator shall add no less than a 3 dB margin for vibration, 4.5 dB for shock, and plus and minus 11°C for thermal range to each maximum predicted environment identified through analysis.

(2) For a new launch vehicle or for a launch vehicle for which there is no empirical data available or empirical data for fewer than three flights, a launch operator shall monitor launch vehicle flight environments with telemetry to verify each maximum predicted environment. A launch operator shall ensure that each maximum predicted environment for any future launch is adjusted to reflect the flight data obtained through monitoring. A launch operator's post-launch report, submitted in accordance with § 417.117(h), must contain the results of any flight environment monitoring performed to verify the maximum predicted environments.

(3) A launch operator shall monitor each transportation, storage, launch processing, and system checkout environment, and adjust the associated maximum predicted environments to reflect the true environments.

(4) The launch operator shall notify the FAA of any change to any maximum predicted environment.

§ 417.309 Command destruct system.

(a) A flight termination system must include a command destruct system that is initiated by radio command and meets the redundancy and other component requirements provided in appendix D of this part. Redundant radio command receiver decoders must be installed on or above the last propulsive launch vehicle stage or payload capable of reaching a populated or other protected area before orbital insertion.

(b) The initiation of a command destruct system must result in accomplishing all flight termination system functions in accordance with § 417.303.

(c) A command destruct system must operate with a radio frequency input signal that has an electromagnetic field intensity of 12 dB below the intensity provided by a command control system transmitter over 95 percent of the radiation sphere surrounding a launch vehicle at any point along the launch vehicle's trajectory.

(d) The design of a command destruct system must provide for the command destruct system to survive the breakup of the launch vehicle to the point that all flight termination functions would be accomplished in accordance with § 417.303. Otherwise, the stage containing the command destruct system must also include an inadvertent separation destruct system implemented in accordance with § 417.311. A launch operator shall perform a breakup analysis in accordance with § 417.329 to demonstrate the survivability of a command destruct system.

(e) A command destruct system must receive and process a valid arm command before accepting a destruct command and destroying the launch vehicle. For any liquid propellant, a command destruct system must non-destructively shut down any thrusting liquid engine as a prerequisite for destroying the launch vehicle.

§ 417.311 Inadvertent separation destruct system.

(a) Each stage or strap-on motor capable of reaching a populated or other protected area before orbital insertion, and which does not possess its own complete command destruct system, including command destruct receivers and associated radio frequency hardware, must be equipped with an inadvertent separation destruct system. An inadvertent separation destruct system is an automatic destruct system that uses mechanical means to trigger the destruction of a stage. If a command destruct system on a stage does not satisfy the requirement of § 417.309(d) that the command destruct system survive breakup of the launch vehicle, a launch operator must also use an inadvertent separation destruct system on that stage.

(b) The initiation of an inadvertent separation destruct system must result in accomplishing all flight termination system functions required by § 417.303 and that apply to the stage or strap-on motor on which it is installed.

(c) An inadvertent separation destruct system must be activated by a device that senses launch vehicle breakup or premature separation of the stage or strap-on motor on which it is located.

(d) An inadvertent separation destruct system must be located to survive during launch vehicle breakup and to ensure its own activation. A launch operator shall perform a flight termination system survivability analysis that accounts for breakup of the launch vehicle and the timing of planned launch vehicle staging events. The analysis shall be used to determine the method of activation and location of an inadvertent separation destruct system that will ensure its survivability and activation during breakup of the launch vehicle.

(e) An electrically initiated inadvertent separation destruct system must have a dedicated power source that supplies the energy to initiate the destruct ordnance.

§ 417.313 Flight termination system safing and arming.

(a) *General.* The design of a flight termination system must provide for safing and arming of all flight termination system ordnance through the use of ordnance initiation devices or arming devices, also referred to as safe and arm devices, that provide a removable and replaceable mechanical barrier or other positive means of interrupting power to each of the ordnance firing circuits to prevent inadvertent initiation of ordnance.

(b) *Flight termination system arming.* The design of a flight termination system must provide for each flight termination system ordnance initiation device or arming device to be armed prior to arming any launch vehicle or payload propulsion ignition circuits. For a launch where propulsive ignition occurs after first motion of the launch vehicle, the design of a flight termination system must provide an ignition interlock that prevents the arming of any launch vehicle or payload propulsion ignition circuits unless all flight termination system ordnance initiation devices and arming devices are armed.

(c) *Preflight safing.* The design of a flight termination system must provide for remote and redundant safing of all flight termination system ordnance initiation devices and arming devices before launch and in case of launch abort or recycle operations.

(d) *In-flight safing.* If flight termination system ordnance is to be safed after a stage or strap-on motor is spent, attains orbit, or can no longer reach any populated or other protected area, the flight termination system safing design must provide for the following:

(1) Any onboard launch vehicle hardware or software used to automatically safe flight termination system ordnance must be single fault tolerant against inadvertent safing. An automatic safing design must satisfy the following:

(i) Any automatic safing must depend on at least two independent parameters, such as time of flight or altitude. The safing criteria for each independent parameter must ensure that the flight termination system on a stage or strap-on-motor can only be safed once the stage or strap-on motor attains orbit or can no longer reach a populated or other protected area.

(ii) An automatic safing design must ensure that all flight termination system ordnance initiation devices and arming devices remain armed during flight until the safing criteria for at least two independent parameters are met.

(iii) If a launch operator proposes to establish any single safing criterion as a value that may be achieved before normal thrust termination of the associated stage or strap-on motor, a launch operator shall demonstrate to the FAA, through the licensing process, that the greatest remaining thrust, assuming a three-sigma high engine performance, can not result in the stage or strap-on motor reaching a populated or other protected area.

(2) If a command destruct system is to be safed by radio command, the command control system used for in-flight safing must be single fault tolerant against inadvertent safing. A launch operator shall implement operational procedures to ensure that launch support personnel do not safe a flight termination system by radio command until the launch vehicle attains orbit or can no longer reach any populated or other protected area.

(e) *Safe and arm monitoring.* The design of a flight termination system must provide for remote monitoring of the safe and arm status of each flight termination system ordnance initiation device and arming device. Safe and arm monitoring circuits must comply with appendix D of this part.

§ 417.315 Flight termination system testing.

(a) *General.* A launch operator shall use flight termination system components that satisfy the qualification, acceptance, and age surveillance test requirements provided in appendix E of this part and any other test requirements established during the licensing process. In addition, a flight termination system and its components shall be subjected to preflight tests in accordance with § 417.317.

(b) *Test plans.* For each launch, a launch operator shall implement written test plans and procedures that specify the test parameters, including pass/fail criteria, for each test and the testing sequence required by appendix E of this part for the applicable component. A launch operator shall also implement test plans for the preflight tests required by § 417.317. Upon review of a proposed launch, the FAA may identify and require additional testing needed to address any unique flight termination system design or operational environment.

(c) *Performance variation.* All performance parameters measured during component testing shall be documented for comparison to previous and subsequent tests to identify any performance variations that may indicate potential workmanship or defects that could lead to a failure of the component during flight.

(d) *Testing of piece parts.* All electronic piece parts used in a flight termination system or a flight termination system component must be tested in accordance with appendix F of this part.

(e) *Visual inspection.* Visual inspections for workmanship and physical damage must be performed before and after each test.

(f) *Test reports.* A launch operator shall prepare test reports for each launch. A test report must document all flight termination system test results and test conditions. Also, any analysis performed in lieu of testing shall be documented in a test report. The test results must be traceable to each applicable system and component using serial numbers or other identification. A test report must include any data that represents ''family characteristics'' to be used for comparison to subsequent tests of components and systems. Any test failure or anomaly, including any variation from an established performance baseline, must be documented with a description of the failure or anomaly, each corrective action taken, and all results of additional tests. Each test report must include a signed statement by each person performing the test and any analysis, attesting to the accuracy and validity of the results.

(1) *Qualification test reports.* A launch operator shall submit all qualification test reports to the FAA no later than six months prior to the first flight attempt. For subsequent launches of the same launch vehicle, a launch operator shall submit qualification test reports for any changes to the flight termination system.

(2) *Acceptance, age surveillance, and preflight test reports.* A launch operator shall submit a summary of each acceptance and age surveillance test no later than 30 days prior to the first flight attempt for each launch. The summary must identify when and where the tests were performed and provide the results. Complete acceptance, age surveillance, and preflight test reports shall be made available to the FAA upon request. A launch operator shall immediately report any failure of a preflight test to the FAA. The resolution of a preflight test failure must be approved by the FAA through the licensing process prior to flight.

(g) *Redesign and retest.* In the case of a redesign of a component due to a failure during testing, all previous tests applicable to the redesign shall be repeated unless the launch operator demonstrates that other testing achieves an equivalent level of safety.

(h) *Configuration management and control.* A launch operator shall ensure that a flight termination system component's manufactured parts, materials, processes, quality controls, and procedures are standardized and maintained in accordance with the launch operator's configuration management and control plan submitted during the licensing process according to § 415.119(e) of this chapter. A launch operator shall ensure that subsequent production items are identical to the components subjected to qualification testing. If there is a change in the design of a qualified component, including any change in a component's parts, the component must be re-qualified in accordance with appendix E of this part.

§ 417.317 Flight termination system preflight testing.

(a) *General.* A launch operator shall conduct preflight flight termination system testing at the component level and the system level in accordance with this section and the applicable requirements provided in § 417.315.

(b) *Preflight component tests.* Preflight component tests shall be conducted at the launch site after qualification and acceptance testing to detect any change in performance that may have resulted from shipping, storage, or other environments that may have affected performance. Performance parameter measurements shall be made during preflight component tests and compared to the acceptance test performance baseline to identify any performance variations, including out-of-family data, which may indicate potential defects that could result in an in-flight failure. Preflight component tests shall be conducted in accordance with this section.

(c) *Batteries.* Each flight termination system battery shall be tested as follows:

(1) The preflight activation and testing of a flight termination system battery prior to installation on a launch vehicle shall include:

(i) Any acceptance testing not previously completed.

(ii) Open circuit testing of each flight termination system battery and each battery cell.

(iii) Load testing of each completed battery assembly.

(iv) Testing of continuity and isolation of each connector.

(v) For manually activated batteries, the pin to case voltage shall be tested to ensure no electrolyte spillage during activation.

(2) A launch operator shall ensure that the time interval between preflight activation and testing of a battery and flight does not exceed the battery's operating life stand time capability.

(3) Battery activation processes and procedures shall be identical to those used during qualification testing.

(4) The preflight testing of a nickel cadmium battery prior to installation shall satisfy the following requirements and in the following order:

(i) The battery shall be initially charged at a rate equal to the battery amp hour capacity divided by 20 (C/20 rate) for 2 hours and then further charged at a C/10 rate for 15 hours.

(ii) The battery shall then be discharged at a C/2 rate to 0.9 volts per cell battery voltage, then discharged at C/10 rate until the first cell reaches 0.1 volts.

(iii) The battery shall then be discharged across a resistor with resistance in ohms equal to the number of cells in the battery times 10 divided by the first battery amp hour capacity until the first battery cell reaches 0.05 volts.

(iv) The battery shall then be recharged at 20 ±5 °C and at a C/10 rate for 16 hours.

(v) The battery shall then be subjected to 20 °C capacity and overcharge testing for 3 cycles.

(vi) The battery shall then be subjected to capacity retention and final impedance and pulse voltage determination at 20 °C and then discharged at −10 °C for 1 cycle.

(d) *Preflight testing of a safe and arm device that has an internal electro-explosive device.* An internal electro-explosive device in a safe and arm device shall undergo preflight testing in accordance with the following:

(1) Preflight testing shall be performed no earlier than 10 calendar days before flight.

(2) Preflight testing must include visual checks for signs of physical defects.

(3) Preflight testing must include safing and arming each device and performing continuity and resistance checks of the electro-explosive device circuit in both the arm and safe position.

(e) *Preflight testing for an external electro-explosive device.* An external electro-explosive device in a safe and arm device shall undergo preflight testing in accordance with the following:

(1) Preflight testing shall be performed no earlier than 10 calendar days before flight.

(2) Preflight testing must include visual checks for signs of physical defects and resistance checks of the electro-explosive device.

(f) *Preflight testing for an exploding bridgewire firing unit.* An exploding bridgewire firing unit must undergo preflight testing in accordance with the following:

(1) Preflight testing shall be performed no earlier than 10 calendar days before flight.

(2) Preflight testing must include verification of bridgewire continuity.

(3) Where applicable, preflight testing shall include high voltage static and dynamic gap breakdown voltage tests.

(g) *Preflight testing for command destruct receivers and other electronic components.* Electronic components shall include any flight termination system component that contains piece part circuitry such as a command destruct receiver. A launch operator shall conduct preflight testing of a command destruct receiver or other electronic component in accordance with the following:

(1) Preflight testing shall be accomplished no earlier than 180 calendar days prior to flight. If the 180-day period expires before flight, an installed electronic component must either be replaced by one that meets the 180-day requirement or tested in place in accordance with an alternate preflight test plan that must be approved by the FAA, through the licensing process, prior to its implementation.

(2) Preflight testing must measure all performance parameters at ambient temperature. The test procedures must satisfy the requirements of appendix E of this part.

(3) Acceptance tests may be substituted for the preflight tests if the acceptance tests are performed no earlier than 180 calendar days prior to flight.

(h) *Preflight subsystem and system level tests.* A launch operator shall conduct preflight subsystem and system level tests of the flight termination system after its components are installed on a launch vehicle to ensure proper operation of the final subsystem and system configurations. Data obtained from these tests shall be compared for consistency to the preflight component tests and acceptance test data to ensure there are no discrepancies indicating a flight reliability concern. Preflight subsystem and system level tests shall be in accordance with the following:

(1) Antennas and associated radio frequency systems shall be tested once installed in their final flight configuration to verify that the voltage standing wave ratio and any insertion losses are within the design limits.

(2) A launch operator shall perform a system level radio frequency preflight test from each command control system transmitter antenna used for the first stage of flight to each command receiver no earlier than 90 days before flight to validate the final integrity of the radio frequency system. These tests shall include calibration of the automatic gain control signal strength curves, verification of threshold sensitivity for each command, and verification of operational bandwidth.

(3) A launch operator shall perform end-to-end tests on all flight termination system subsystems, including command destruct systems and inadvertent separation destruct systems. End-to-end tests shall be performed no earlier than 72 hours before the first flight attempt. If the flight is delayed more than 14 calendar days or the flight termination system configuration is broken or modified for any reason, such as to

replace batteries, the end-to-end tests shall be repeated no earlier than 72 hours before the next flight attempt. A launch operator shall perform end-to-end tests with the flight termination system in its final onboard launch vehicle configuration except for the ordnance initiation devices. End-to-end tests must incorporate the following:

(i) A destruct initiator simulator that satisfies § 417.327 shall be installed in place of each flight initiator to verify that the command destruct and inadvertent separation destruct systems deliver the energy required to initiate flight termination system ordnance.

(ii) All flight termination systems shall be powered by the batteries that will be used for flight. A flight termination system battery shall not be recharged at any time during or after end-to-end testing. If the battery is recharged at any time before flight the entire end-to-end test shall be performed again.

(iii) All command destruct receiver commands shall be exercised using the command control system transmitters in their flight configuration.

(iv) All primary and redundant flight termination system components, circuits and command control system transmitting equipment shall be verified as operational.

(v) The triggering mechanism of all electrically initiated inadvertent separation destruct systems shall be exercised and verified as operational.

(4) An open-loop radio frequency test shall be performed, no earlier than 60 minutes prior to flight, to validate the entire radio frequency command destruct link. This test shall be performed in accordance with the following:

(i) All flight termination system ordnance initiation devices must be in a safe condition.

(ii) Flight batteries must power all receiver decoders and other electronic components. The launch operator shall ensure that the testing allows for any warm-up time needed to ensure the reliable operation of electronic components.

(iii) All receiver decoder commands except destruct shall be exercised open loop from the command control transmitters.

(iv) All receiver decoders and all command control transmitters shall be tested and verified as operational.

(5) If the integrity of a subsystem or system is compromised due to a configuration change or other event, such as a lightning strike or inadvertent connector mate or de-mate, the associated preflight subsystem or system testing shall be repeated.

§ 417.319 Flight termination system installation procedures.

(a) A launch operator shall implement written procedures to ensure that flight termination system components, including electrical components and ordnance, are installed on a launch vehicle in accordance with the flight termination system design. These procedures must ensure that:

(1) All personnel involved are qualified for the task in accordance with § 417.105.

(2) The installation of all flight termination system mechanical interfaces is complete.

(3) Qualified personnel use calibrated tools to install ordnance when a specific standoff distance is necessary to ensure that the ordnance has the desired effect on the material it is designed to cut or otherwise destroy.

(b) Flight termination system installation procedures must include, but need not be limited to the following:

(1) A description of each task to be performed, each facility to be used, and each and any hazard involved.

(2) A checklist of tools and equipment required.

(3) A list of personnel required for performing each task.

(4) Step-by-step directions written with sufficient detail for a qualified person to perform each task. The directions must identify any tolerances that must be met during the installation.

(5) Steps for inspection of installed flight termination system components, including quality assurance oversight procedures.

(6) A place for the personnel performing the procedure to initial or otherwise signify that each step is accomplished and for recording the outcome and any data verifying successful installation.

§ 417.321 Flight termination system monitoring.

(a) A launch operator shall ensure that the following data is available through monitoring to determine the status of a flight termination system prior to and during flight:

(1) The signal strength telemetry output voltage for the command destruct receiver.

(2) All command destruct receiver outputs commands.

(3) Status of each ordnance initiation device, whether in the arm or safe position.

(4) Voltage monitoring for each flight termination system battery.

(5) Current monitoring for each flight termination system battery.

(6) Status of any special electrical inhibits within the flight termination system.

(7) Parameters of each high energy firing unit, such as arm input, power, firing capacitor and trigger capacitor.

(8) Electrical inadvertent separation destruct system safe, arm, and destruct output command status.

(9) Temperature monitoring of each flight termination system battery.

(10) Power switch status, whether on internal or external power.

(11) Environmental monitoring needed to verify each maximum predicted environment required by § 417.307 and appendix D of this part.

(b) Monitor consoles must include all communications and monitoring capability necessary to ensure that the status of a flight termination system can be ascertained and relayed to the appropriate launch officials.

(c) A launch operator shall establish pass/fail flight commit criteria in accordance with § 417.113 for monitored flight termination system parameters to support launch abort decisions and to ensure a flight termination system is performing as required at the time of flight. The flight commit criteria shall be incorporated in a launch operator's launch plans as submitted to the FAA through the licensing process.

§ 417.323 Command control system requirements.

(a) *General.* A launch operator shall employ a command control system as part of a flight safety system. A command control system must consist of the flight safety system elements that ensure that a command signal will be transmitted if needed during the flight of a launch vehicle and received by the onboard vehicle flight termination system. A command control system, including all subsystems and support equipment, must satisfy the requirements of this section and must include, but need not be limited to the following:

(1) All flight termination system activation switches at a flight safety official console;

(2) All intermediate equipment, linkages, and software;

(3) Any auxiliary stations;

(4) Each command transmitter and transmitting antenna; and

(5) All support equipment that is critical for reliable operation such as power, communications, and air conditioning systems.

(b) *Compatibility.* A launch operator's command control system must be compatible with the flight termination system onboard the launch operator's launch vehicle. A launch operator shall demonstrate compatibility through analysis and testing in accordance with

§ 417.315, § 417.325, D417.15 of appendix D of this part, and E417.19 of appendix E of this part.

(c) *Reliability design.* A command control system must have a reliability design of 0.999 at a confidence level of 95 percent. A launch operator shall perform a system reliability analysis in accordance with § 417.329 to demonstrate whether a command control system satisfies this requirement. The reliability analysis must demonstrate the command control system's reliability when operating for the time period from completion of preflight testing and system verification performed in accordance with § 417.325(c) through initiation of flight and until the no longer endanger time determined in accordance with § 417.221(c). In addition, a launch operator's command control system must satisfy the following:

(1) A command control system must not contain any single-failure-point that, upon failure, would inhibit the required functioning of the system or cause the transmission of an undesired flight termination message.

(2) A command control system's design must ensure that the probability of transmitting an undesired or inadvertent command during flight is less than 1×10^{-7}.

(d) *Command control system delay time.* A command control system's radio message delay time, from initiation of a flight termination command at the flight safety official console to transmission from the command transmitter antenna, must be sufficiently low to complete the transmission of the command destruct sequence of signal tones prior to an errant launch vehicle exiting the 3–dB point of the command antenna pattern.

(e) *Configuration management and control.* The configuration of a command control system must be controlled in accordance with the launch operator's configuration management and control plan submitted during the licensing process according to § 415.119(e).

(f) *Electromagnetic interference.* Each command control system component must be designed and qualified to function within the electromagnetic environment to which it will be exposed. A command control system must include electromagnetic interference protection to prevent any electromagnetic interference from inhibiting the required functioning of the system or causing the transmission of an undesired flight termination command. Electromagnetic interference protection must also be provided for any susceptible remote control data processing and transmitting systems that are part of the command control system.

(g) *Command transmitter failover.* A command control system must include independent, redundant transmitter systems that automatically switch or "fail-over" from a primary transmitter to a secondary transmitter when a condition exists that indicates potential failure of the primary transmitter. The switch must be automatic and provide all the same command control system capabilities through the secondary transmitter system. The secondary transmitter system must respond to any transmitter system configuration and radio message orders established for the launch. A launch operator shall establish and implement fail-over criteria that trigger automatic switching from the primary transmitter system to the secondary system during any period of flight up to the no longer endanger time. A launch operator's fail-over criteria must account for each of the following transmitter performance parameters and failure indicators:

(1) Low transmitter power,

(2) Center frequency shift,

(3) Tone deviation,

(4) Out of tolerance tone frequency,

(5) Out of tolerance message timing,

(6) Loss of communication between central control and transmitter site,

(7) Central control commanded status and site status disagree,

(8) Transmitter site fails to respond to a configuration or radiation order within a specified period of time, and

(9) Tone imbalance.

(h) *Radio carrier illumination.* A command control system must be capable of providing the radiated power density that a flight termination system would need to activate during flight and in accordance with § 417.309(c). A launch operator shall ensure that manual or automatic switching between transmitter systems, including fail-over, does not result in the radio carrier being off the air long enough for the airborne flight termination system to be captured by some other unauthorized transmitter. This includes any loss of carrier and any simultaneous multiple radio carrier transmissions from two transmitter sites during switching.

(i) *Command control system monitoring and control.* A command control system must be capable of being controlled and monitored from the flight safety official console and the transmitter sites in accordance with § 417.327(g). A command control system's design must allow for real-time selection of a transmitter, transmitter site, communication circuits, and antenna configuration. A launch operator shall establish procedures for sending commands from the transmitter sites in the event of a failure of the flight safety official console.

(j) *Transmitter system.* A command control transmitter system must:

(1) Transmit signals that are compatible with the airborne flight termination system in accordance with D417.15 of appendix D of this part.

(2) Ensure that commands transmitted to a flight termination system have priority over any other commands transmitted.

(3) Employ an authorized radio carrier frequency and bandwidth.

(4) Not transmit a signal that could interfere with other airborne flight termination systems on other launch vehicles that may operate from the same launch site. A launch operator shall coordinate with any launch site operator and other launch operators to ensure this requirement is met.

(5) Transmit an output bandwidth that is consistent with the signal spectrum power used in the launch operator's link analysis performed in accordance with § 417.329(h).

(6) Not transmit other frequencies that could degrade the airborne flight termination system's performance. Any spurious signal levels must be at least 60 dB below the radio frequency output signal level from the transmitter antenna.

(7) Ensure that all requirements of this section are satisfied during application and removal of tone frequencies.

(k) *Command control system antennas.* A command control system antenna or system of antennas must provide command signals to a flight termination system throughout normal and non-nominal launch vehicle flight regardless of launch vehicle orientation and must satisfy the following:

(1) An antenna must have a beam-width that allows sufficient reaction time to complete the transmission of the command destruct sequence of signal tones prior to an errant launch vehicle exiting the 3–dB point of the antenna pattern. The beam-width and associated reaction time must account for the pointing accuracy of the antenna. The antenna beam-width must encompass the normal flight trajectory boundaries for the portion of flight that the antenna is scheduled to support.

(2) Each antenna must be located to achieve line of site between the antenna and the launch vehicle during the portion of flight that the antenna is scheduled to support.

(3) An antenna system must provide a continuous omni-directional radio carrier illumination pattern that covers the launch vehicle's flight from the launch point to no less than an altitude

of 50,000 feet above sea level unless the launch operator demonstrates, clearly and convincingly, through the licensing process that an equivalent level of safety can be achieved with a steerable antenna for that portion of flight.

(4) An antenna must radiate circularly polarized radio waves that are compatible with the flight termination system antennas on the launch vehicle.

(5) A steerable antenna must be controlled manually at the antenna site or by remote slaving data from a launch vehicle tracking source.

(6) A steerable antenna must be capable of supplying the required power density in accordance with paragraph (h) of this section to the flight termination system on the launch vehicle for the portion of flight that the antenna is scheduled to support. A steerable antenna's positioning lag, accuracy, and slew rates must allow for tracking a launch vehicle during nominal flight within one half of the antenna's beam width and for tracking of an errant launch vehicle to ensure that the delay time and beam-width requirements of paragraphs (d) and (k)(1) of this section are satisfied. A launch operator shall ensure that the worst-case power loss due to antenna pointing inaccuracies is factored into the radio frequency link analysis performed in accordance with § 417.329(h).

§ 417.325 Command control system testing.

(a) *General.* A command control system, its subsystems, and components must undergo acceptance and preflight tests in accordance with the requirements of this section. A launch operator shall ensure that testing of a command control system is conducted in accordance with the following:

(1) Each test shall be conducted in accordance with a written test plan that specifies the procedures and test parameters for the test and the testing sequence to be followed. A test plan must include instructions on how to handle procedural deviations and how to react to test failures.

(2) Visual inspections for workmanship and physical damage shall be performed before and after each test.

(3) When a component is replaced or redesigned, all previous acceptance and preflight tests shall be repeated.

(4) Modifications to command control system hardware and software shall be validated with end to end regression testing.

(5) Compatibility of the command control system with a launch vehicle's onboard flight termination system shall be tested independently and as part of preflight testing.

(b) *Acceptance testing.* All new or modified command control system hardware and software must undergo acceptance testing to verify that the system meets the functional and performance requirements in § 417.323. Acceptance testing shall include system interface validation, integrated system-wide validation, and must satisfy the following:

(1) All new or modified command control system hardware and software shall be validated using a system acceptance test plan. A system acceptance test plan shall include testing of the new components or subsystems, system interface validation, and integrated system wide validation. The system acceptance test plan and the results of the acceptance testing shall both be reviewed by and signed as accurate by the launch operator's launch safety official.

(2) A launch operator shall ensure that a failure modes and effects analysis is performed for the design of each new system and any modification to an existing system.

(3) Computing systems and software testing must satisfy the requirements of § 417.123 and appendix H of this part.

(4) A launch operator shall ensure that testing is performed to measure and validate the command control system performance parameters contained in § 417.323.

(c) *Preflight testing.* A command control system shall undergo preflight testing in coordination with preflight testing of an associated flight termination system and must satisfy the requirements of § 417.317. In addition, preflight tests of a command control system to be performed in preparation for the coordinated flight termination system tests must satisfy the following requirements:

(1) *Auto carrier tests.* A launch operator shall verify that, for any auto carrier switching system, the switching algorithm selects the proper transmitter site and the auto carrier switching system enables the selected site. This test may be conducted simultaneously with any theoretical data run. This test shall be performed no earlier than four hours before a scheduled flight time.

(2) *Command transmitter switching tests.* A launch operator shall perform an open loop end-to-end verification test of each element of a command control system from the flight safety official console to each command transmitter site to verify the integrity of the overall system. A launch operator shall ensure that successful verification is performed for each flight safety official console and remote command transmitter site combination. The verification must be initiated by transmitting all functions programmed for the launch from the flight safety control console. The verification shall be concluded at each command transmitter site by operator confirmation that the proper function commands were received. This test may be performed simultaneously with the independent radio frequency open loop validation required by paragraph (c)(3) of this section. A launch operator shall conduct switching tests in accordance with the following:

(i) The verification shall be conducted as close to the planned flight time as operationally feasible and must be repeated in the event that the command control system configuration is broken or modified before launch.

(ii) All measurements will be repeated for each flight safety official console and remote command site combination, for all strings and all operational configurations of cross-strapped equipment.

(3) *Independent radio frequency open loop verification tests.* A launch operator shall perform an open loop end-to-end verification of each element of a command control system from the flight safety official console to each command transmitter site to quantitatively verify the quality of the transmitted information. This verification must be performed for each flight safety official console and remote command transmitter site combination. The verification shall be initiated by transmitting all functions programmed for the launch from the flight safety control console. The verification shall be concluded, at each command site, by measuring all applicable parameters received and transmitted with analysis equipment that does not physically interface with any elements of the operational command control system. This verification may be performed simultaneously with the switching tests required by paragraph (c)(2) of this section. A launch operator shall conduct open loop end-to-end verification tests in accordance with the following:

(i) The verification shall be conducted as close to the planned launch time as operationally feasible and must be repeated in the event that the command control system configuration is broken or modified before launch.

(ii) Test equipment must be capable of validating transmission of the required parameters.

(iii) All measurements shall be repeated for each flight safety official console and remote command transmitter site combination, for all strings and all operational configurations of cross-strapped equipment.

(iv) The test code used for arm and destruct shall include at least one occurrence of each tone programmed for the specific mission.

(v) The testing must verify that all critical command control system performance parameters are within their performance specifications. These parameters include, but need not be limited to:

(A) Transmitter power output,

(B) Center frequency stability,

(C) Tone deviation,

(D) Tone frequency,

(E) Message timing,

(F) Status of communication circuits between the flight safety official console and any supporting command transmitter sites,

(G) Status agreement between the flight safety official console and any supporting command transmitter sites,

(H) Fail-over conditions, and

(I) Tone balance.

(d) *Test reports.* A launch operator shall prepare test reports on command control system testing for each launch. A test report must document all command control system test results and test conditions. Also, any analysis performed in lieu of testing shall be documented in the test report. The test results must be traceable to each applicable system and component using serial numbers or other identification. Any test failure or anomaly, including any variation from an established performance baseline, must be documented with a description of the failure or anomaly, each corrective action taken, and all results of additional tests. A test report must identify any test failure trends. Each test report must include a signed statement by each person performing the test and any analysis, attesting to the accuracy and validity of the results. A launch operator shall submit an acceptance-test report summary to the FAA no later than 30 days prior to the first flight attempt. Any failure of a preflight test shall be reported to the FAA immediately. Resolution of all failures must be documented and approved by the FAA through the licensing process prior to flight.

§ 417.327 Support systems.

(a) *General.* A flight safety system must consist of compatible launch vehicle tracking, visual data source, telemetry, communications, data display, and data recording systems that support the flight safety official. Each support system must have written performance specifications that contain the particulars of how the system functions and satisfies the requirements of this section. For each launch, a launch operator shall perform tests of each support system to ensure it functions in accordance with its performance specifications.

(b) *Launch vehicle tracking.* A flight safety system must include a launch vehicle tracking system that provides continuous launch vehicle position and status data to the flight safety official from liftoff through the time that the launch vehicle reaches orbit or can no longer reach any protected area. A launch vehicle tracking system for a launch that employs a flight safety system must satisfy the following requirements:

(1) A tracking system must consist of two sources of valid launch vehicle position data. The two data sources must be independent of one another, and at least one source must be independent of any system or component associated with determining or measuring vehicle position or performance used to aid the vehicle guidance system unless the launch operator demonstrates, clearly and convincingly, through the licensing process that another approach, such as the use of redundant vehicle guidance units, provides an equivalent level of safety for the launch.

(2) All ground tracking systems and components must be compatible with the tracking system components onboard the launch vehicle.

(3) When a flight safety system uses radar as an independent tracking source, the vehicle must have a tracking beacon onboard the launch vehicle unless the launch operator provides a clear and convincing demonstration through the licensing process that any skin tracking maintains a tracking margin of no less than six dB above noise throughout the period of flight that the radar is used and that the flight control lines and flight safety limits account for the larger tracking errors associated with skin tracking.

(4) Tracking system data must be provided to the flight safety official through the flight safety data display system at the flight safety official console.

(5) A tracking system must verify the accuracy of any launch vehicle tracking data provided to the flight safety official during flight. A tracking source that is independent of any system used to aid the launch vehicle guidance system shall validate launch vehicle guidance data before a flight safety official uses the launch vehicle guidance data as a source of tracking data in the flight termination decision process.

(c) *Visual tracking.* A flight safety system must include launch vehicle observers stationed at program and back azimuth positions to provide flight status data to the flight safety official at liftoff and during the early seconds of flight. A launch operator shall ensure that each launch vehicle observer meets the requirements of § 417.331(i) and § 417.331(j). Skyscreens or other visual data sources operated by a launch vehicle observer may be used as part of a launch operator's flight safety system.

(d) *Telemetry system.* A flight safety system must include a telemetry system that provides continuous, accurate flight safety data during preflight operations, lift-off, and during flight until the launch vehicle reaches orbit or can no longer reach any populated or other protected area. A telemetry system must meet the following requirements:

(1) An onboard telemetry system must monitor and transmit data to the flight safety official console regarding the following:

(i) Inertial measurement data from vehicle guidance and control.

(ii) Vehicle flight performance data, including motor chamber pressure and thrust vector control data.

(iii) Status of onboard tracking system components.

(iv) All flight termination system monitoring data in accordance with § 417.321.

(2) A telemetry receiving system must acquire, store, and provide real time data to the flight safety official for any flight termination decision.

(3) A telemetry system must provide data to the flight safety official at the flight safety official console through the flight safety data processing system.

(e) *Communications system.* A flight safety system must include a communications network that connects all flight safety functions with all launch control centers and any down range tracking and command transmitter sites. A flight safety system must provide for recording all data and voice communications channels during launch countdown and flight.

(f) *Flight safety data processing, display, and recording system.* A flight safety system must include a flight safety data processing system that processes data for display and recording to support the flight safety official's monitoring of the launch. A flight safety data processing system must:

(1) Receive vehicle status data from tracking and telemetry, evaluate the data for validity, and provide valid data for display and recording.

(2) Perform any reformatting of the data as appropriate and forward it to display and recording devices.

(3) Display real-time data against background displays of the nominal trajectory and flight safety limits established in accordance with the flight safety analysis required by subpart C of this part.

(4) Display and record raw input and processed data at 0.1-second intervals.

(5) Record the timing of when flight safety system commands are input by the flight safety official or other flight safety crewmembers.

(g) *Flight safety official console.* A flight safety system must include a flight safety official console that contains the flight safety displays and controls used by a flight safety official. A flight safety official console must provide for monitoring and evaluating launch vehicle performance, provide for communications with other flight safety and launch personnel, and must contain the controls for initiating flight termination.

(1) Data displayed on a flight safety official console must include, but need not be limited to, the following:

(i) Instantaneous vacuum impact point or drag corrected debris footprint by tracking and telemetry state vectors.

(ii) Present launch vehicle position and velocities as a function of time.

(iii) Vehicle status data from telemetry, including yaw, pitch, roll, and motor chamber pressure.

(iv) Flight termination system battery levels and receiver gain in relation to receiver sensitivity.

(v) Displays of nominal trajectory, flight safety limits, minimum time to endanger, no longer endanger time, and any overflight gate through a flight control line as determined by the launch operator's flight safety analysis performed in accordance with subpart C of this part.

(vi) Displays of any video data to be used by the flight safety official such as video from optical program and flight line cameras.

(2) A flight safety official console must allow a flight safety official to turn a command transmitter on and off, manually switch from primary to backup transmitter antenna and switch between any transmitter sites. These functions shall be accomplished through controls at the flight safety official console or through communications links at the console between the flight safety official and command transmitter support personnel.

(3) A flight safety official console must include a means of identifying to a flight safety official when the console has primary control of a command transmitter system.

(4) A flight safety official console must provide a means of readily identifying whenever an automatic fail-over of the system transmitters has occurred.

(5) A flight safety official console must be dedicated to the flight safety system and must not rely on time or equipment shared with other systems.

(6) A flight safety official console's inherent delay from message initiation to transmission of the message leading edge must be no more than 55 milliseconds.

(7) All data transmissions links between the console and each transmitter and antenna must consist of two or more complete and independent duplex circuits. These circuits must be routed so that they are physically separated from each other to eliminate any potential single failure point in the command control system in accordance with § 417.323(c)(1).

(8) A launch operator shall employ hardware and procedural security provisions for controlling access to the flight safety official console and other related hardware. These security provisions must ensure no person or system can initiate a flight safety system transmission, either deliberately or inadvertently, unless the transmission is ordered by the flight safety official.

(9) There must be two independent means for the flight safety official to initiate arm and destruct messages. The location and functioning of the controls must provide a flight safety official easy access to the controls and prevent inadvertent activation.

(10) A flight safety official console must include a digital countdown for use in implementing the flight termination rules in accordance with § 417.113 that apply data loss flight times, earliest destruct time, and no longer endanger time determined in accordance with § 417.221. A launch operator shall also provide a manual method of applying the data loss flight times in the event that a flight safety system malfunction prevents the flight control official from viewing a digital countdown of the data loss flight times.

(h) *Support equipment calibration.* A launch operator shall calibrate its support systems and any equipment used to test flight safety system components to ensure that measurement and monitoring devices that support a launch provide accurate indications.

(i) *Destruct initiator simulator.* A launch operator shall use a destruct initiator simulator to simulate a destruct initiator during the flight termination system preflight tests required by § 417.317. This device must have electrical and operational characteristics matching those of the actual destruct initiator. A destruct initiator simulator must:

(1) Monitor the firing circuit output current, voltage, or energy, and latch on when the operating current, voltage, or energy for the initiating device is outputted from the firing circuit.

(2) Remain connected throughout ground processing until the electrical connection of the actual initiators is accomplished.

(3) Include an interlock capability that permits the issuance of destruct commands by test equipment only if the simulator is installed and connected to the firing lines.

(4) For low voltage initiators, provide a stray current monitoring device such as a fuse or automatic recording system capable of indicating a minimum of one tenth of the maximum no-fire current. This stray current monitoring device must be installed in the firing line.

(j) *Timing system.* A launch operator's flight safety system must include a timing system synchronized with the United States Naval Observatory, Washington DC. A launch operator shall use this system to time tag data; initiate first motion signals; synchronize flight safety system instrumentation, including countdown clocks; and time tag recordings of required data and voice communication channels during countdown and flight.

§ 417.329 Flight safety system analysis.

(a) *General.* A launch operator shall perform each system analysis defined by this section to verify that a flight termination system, a command control system, and their components meet the reliability requirements of this subpart. These analyses must be performed following standard industry system safety and reliability analysis methodologies. (Guidelines for performing system safety and reliability analyses may be obtained at http://ast.faa.gov/licensing in FAA Advisory Circular AC 431A, draft available 4/21/99). For each analysis, a launch operator shall prepare an analysis report that documents how the analysis was performed and the findings in accordance with this section.

(b) *System reliability analysis.* A launch operator shall prepare a reliability analysis for the flight termination system and the command control system that demonstrates the analytical reliability of these systems. This analysis shall account for the probability of a flight safety system anomaly occurring and its effects as determined by the fault tree analysis; failure modes, effects, and criticality analysis; and the sneak circuit analysis required by paragraphs (c), (d), and (i) of this section. A launch operator's flight termination system and command control system reliability analysis report must:

(1) Describe how the flight termination system and command control system meet the reliability design requirement of 0.999 at a confidence level of 95 percent.

(2) Provide each reliability model used.

(3) Provide computations on actual or predicted reliability for all subsystems and components.

(4) Describe the effects of storage, transport, handling, maintenance, and operating environments on component reliability.

(5) Describe the interface between the launch vehicle systems and the flight termination system.

(c) *Fault tree analysis.* A launch operator shall perform a fault tree analysis to identify flight termination system paths and command control system paths that could permit an undesired event that would cause the flight safety system to fail to function. A launch operator shall include the probability of occurrence of any undesired event as part of each system's reliability design determination.

(d) *Failure modes effects and criticality analysis.* A launch operator shall perform a failure modes effects and criticality analysis based on failures identified by a fault tree analysis to determine and document all possible failure modes and their effects on flight termination system and command control system performance. The results of a failure modes effects and criticality analysis shall be used as input to the flight safety system reliability analysis. A failure modes effects and criticality analysis must:

(1) Identify all failure modes and their probability of occurrence.

(2) Identify single point failure modes.

(3) Identify areas of design where redundancy is required pursuant to § 417.305.

(4) Identify functions, including redundancy, which are not or cannot be tested.

(5) Provide input to reliability modeling and predictions.

(6) Include any potential system failures due to hardware, software, test equipment, or procedural or human errors.

(e) *Single failure point analysis.* A launch operator shall perform a single failure point analysis to verify that no single failure can cause inadvertent flight termination system activation or disable the flight termination system or command control system.

(f) *Fratricide analysis.* A launch operator shall perform a fratricide analysis to verify that flight termination of a stage will not sever interconnecting flight termination system circuitry or ordnance to other stages until flight termination on the other stages has been initiated.

(g) *Bent pin analysis.* A launch operator shall perform a bent pin analysis for each component to verify that any single short circuit occurring as a result of a bent electrical connection pin shall not result in inadvertent system activation or inhibiting the proper operation of the flight termination system or command control system.

(h) *Radio frequency link analysis.* A launch operator shall perform a radio frequency link analysis of the onboard flight termination system and command control system. This analysis must verify that the system is capable of reliable operation with signals, at the input to the receiver, having electromagnetic field intensity of 12dB below the intensity provided by the command transmitter in accordance with appendix D of this part. A link analysis must include path losses due to plume or flame attenuation, aspect angle, vehicle trajectory, ground system radio frequency characteristics, worst-case power loss due to antenna pointing inaccuracies, and any other attenuation factors. Guidelines for performing a radio frequency link analysis are provided in Range Commanders Council Standard 253 and may be obtained from the FAA (http://ast.faa.gov/licensing).

(i) *Sneak circuit analysis.* A launch operator shall perform a sneak circuit analysis to identify latent paths of an unwanted command that could, when all components are otherwise functioning properly, cause the occurrence of undesired, unplanned, or inhibited functions that could cause a flight termination system or command control system anomaly. The probability of such an anomaly occurring must be incorporated into each system's reliability determination in the system reliability analysis required by paragraph (b) of this section.

(j) *Software and firmware analysis.* A launch operator shall analyze any flight safety system software or firmware that performs a software safety critical function to ensure reliable operation in accordance with appendix H of this part.

(k) *Flight termination system battery capacity analysis.* A launch operator shall perform an analysis to demonstrate that a flight termination system battery has a total amp hour capacity equal to 150% of the capacity that the flight termination system requires to operate during flight plus the capacity needed for load and activation checks, preflight and launch countdown checks, and any potential launch hold time. For a launch vehicle that uses any solid propellant, the battery capacity must allow for an additional 30-minute hang-fire hold time. The battery analysis must also demonstrate each flight termination system battery's ability to meet the charging temperature and current control requirements of appendix D of this part.

(l) *Flight termination system survivability analysis.* A launch operator shall perform a flight termination system survivability analysis that accounts for breakup of the launch vehicle, with and without a commanded flight termination. The analysis shall be used to determine the design and location of the flight termination system components and subsystems. A flight termination system survivability analysis must account for:

(1) Breakup of the launch vehicle due to aerodynamic loading effects at high angle of attack trajectories during early stages of flight.

(2) An engine hard-over nozzle induced tumble during various phases of flight for each stage.

(3) The timing of launch vehicle staging and other events that, when they occur, can result in damaging flight termination system hardware or inhibit the functionality of flight termination system components or subsystems, including any inadvertent separation destruct system.

§ 417.331 Flight safety system crew roles and qualifications.

(a) *General.* Flight safety system hardware must be operated by a flight safety system crew made up of a flight safety official and support personnel possessing the qualifications required by and carrying out the roles defined by this section. A launch operator shall ensure that its flight safety system crewmembers meet the qualification requirements of this section unless the launch operator demonstrates clearly and convincingly through the licensing process that an alternate approach provides an equivalent level of safety. A launch operator shall document each flight safety system crew position description and maintain documentation on individual crew qualifications, experience, and training as part of the personnel certification program required by § 417.105. A flight safety system crewmember may perform the roles of more than one position required by this section for a launch, provided that all the requirements of each role and related tasks are accomplished.

(b) *Flight safety system crew qualifications.* In addition to the qualifications required for specific flight safety system crew positions, all flight safety system crewmembers shall have at least four years experience in safety or a related discipline. The four years of experience must include all of the following:

(1) Two years of experience in launch vehicle or missile operations, aircraft operations, missile or aircraft range operations, or weapons controller operations, while performing duties and functions that require critical real time decision-making.

(2) Knowledge and experience in communications systems and procedures, including both voice and data.

(3) Knowledge and experience in computers, graphical data systems, radar and telemetry real-time data, and flight termination systems.

(4) Training to become familiar with the launch site, launch vehicle, and all applicable flight safety system functions, equipment, and procedures related to a launch before being called upon to support that launch. Each member of the flight safety system crew shall undergo a preflight readiness training program that includes hands-on exercises and simulations of multiple launch scenarios and launch vehicle failure modes.

(c) *Senior flight safety official role.* A launch operator shall designate a senior flight safety official that reports directly to the launch safety director identified in § 417.103, oversees the training and certification of flight safety system crewmembers, defines crew needs for specific launches, and supervises crew performance as follows:

(1) A senior flight safety official shall, during the flight of a launch vehicle, oversee in person the flight safety official's decisions with respect to the flight safety system, including initiation of flight termination. A senior flight safety official may perform as a backup for the flight safety official.

(2) A senior flight safety official shall certify each member of the flight safety system crew for each launch. A senior flight safety official shall develop and implement a certification program that includes:

(i) Mission specific training programs to ensure team readiness.

(ii) Dynamic launch simulation exercises of system failure modes designed to test crew performance, flight termination criteria, and flight safety data displays.

(3) A senior flight safety official shall certify each member of the flight safety system crew as fully qualified when the crewmember is able to perform the functions of a specific crew position for each launch. The senior flight safety official shall:

(i) Verify that a candidate crewmember meets the qualification, training, and performance requirements of the position.

(ii) Identify and implement any additional training, exercises, and refresher training needed to ensure that a crewmember is qualified for each launch.

(d) *Senior-flight safety official qualifications.* A senior flight safety official shall be a qualified flight safety official as described by paragraph (f) of this section with no fewer than three years of flight safety system crew experience. In addition, a senior flight safety official for a specific launch shall have supported or been the flight safety official on at least one prior launch of that or an equivalent launch vehicle.

(e) *Flight safety official role.* A launch operator shall designate a flight safety official for each launch who shall:

(1) Monitor the flight of the vehicle by means of real-time displays of tracking data, including present position and any instantaneous impact point or debris footprint.

(2) Monitor video information, telemetry data, and communications from other flight safety system crewmembers who advise the flight safety official on the status of their task.

(3) Initiate any required flight termination in accordance with the flight termination rules established in accordance with § 417.113.

(f) *Flight safety official qualifications.* In addition to the qualifications required by paragraph (b) of this section, a flight safety official shall have the following knowledge, experience and training:

(1) A bachelors degree in engineering, mathematics, physics or other scientific discipline with equivalent mathematics and physics requirements or equivalent technical experience and education.

(2) Knowledge of the application of safety support systems such as position tracking sources, digital computers, displays, command destruct, communications, and telemetry.

(3) Knowledge of the electrical functions of a flight termination system and understanding of the principles of radio frequency transmission and attenuation.

(4) Knowledge of the behavior of ballistic and aerodynamic vehicles in-flight under the influence of aerodynamic forces.

(5) Experience in missile, space, or aircraft operations requiring real-time decisions in response to changing conditions.

(6) Experience as a certified telemetry safety official as defined in paragraph (g) of this section for at least one launch.

(7) Experience as a certified back azimuth observer as defined in paragraph (i) of this section for at least one launch.

(8) Experience as a certified program observer as defined in paragraph (i) of this section for at least one launch.

(9) Experience, for at least one launch, as an observer of a qualified flight termination system safety official as defined in paragraph (k) of this section.

(10) Experience as an observer and assistant to a qualified flight safety analyst as defined in paragraph (m) of this section on all preparations for at least one launch.

(11) Training on all the components that are involved in the calculation and production of the flight safety displays and the computations of probability of impact and expected casualty. This training shall include the interrelationships and sensitivity of the results to changes in each of the components.

(g) *Telemetry safety official role.* A launch operator shall designate a telemetry safety official for each launch. The safety official shall monitor real-time safety telemetry data from the launch vehicle and advise the flight safety official when normal planned events occur and when any anomalous condition occurs.

(h) *Telemetry safety official qualifications.* In addition to the qualifications required by paragraph (b) of this section, a telemetry safety official shall have the following knowledge, experience, and training:

(1) A working knowledge of telemetry data displays such as strip chart recorders and digital readout systems. A telemetry safety official must know the purpose of each telemetry parameter displayed, know the nominal operating range of each parameter, and recognize anomalous conditions as they occur.

(2) Experience, for at least one launch, as an observer of a qualified telemetry safety official.

(3) Experience performing as a telemetry safety official during training simulations that involve playback of telemetry data on at least three nominal and two failure mission scenarios.

(4) Experience as a telemetry safety official, under the supervision of a qualified telemetry safety official, for at least one launch.

(i) *Launch vehicle observer role.* A launch operator shall designate back azimuth and program launch vehicle observers to establish and remain in visual contact with the launch vehicle during the early portion of flight when the tracking sensors are unable to provide position and predicted impact data to the flight safety official. Vehicle observers shall be in direct communication with, and advise the flight safety official when the launch vehicle engines ignite, the launch vehicle lifts off the pad, and when the launch vehicle pitches over and proceeds downrange. A flight safety system crew shall include, but is not limited to, the following launch vehicle observers:

(1) *Back azimuth observer.* An observer located 180 ± 10 degrees behind the projected launch azimuth.

(2) *Program observer.* An observer located along a line that passes through the launch point and that is perpendicular within ± 10 degrees to the projected launch azimuth.

(j) *Launch vehicle observer qualifications.* In addition to the qualifications required by paragraph (b) of this section, any observer at the back azimuth location and any observer at the program location shall have the following qualifications:

(1) Training in failure modes and how failures would appear to the observer from the observer's location at the time of flight.

(2) Experience observing a qualified launch vehicle observer at the location, for at least one launch.

(3) Experience for at least two launches performing as a launch vehicle observer at the location, under the supervision of a launch vehicle observer qualified at that location.

(k) *Flight termination system safety official role.* A launch operator shall designate a flight termination system safety official for each launch. This person shall monitor the proper installation and testing of the onboard flight termination system prior to flight and determine whether the command control system and the flight termination system are in the proper configuration and functioning properly immediately before flight. A flight termination system safety official shall provide real-time command control system support to the flight safety official during flight of a launch vehicle. The flight termination system safety official shall also coordinate with other flight safety system crewmembers in the development of mission rules, perform vehicle trajectory analysis, determine public protection lines and flight safety limits, and perform the flight safety system analyses required by § 417.329.

(l) *Flight termination system safety official qualifications.* In addition to the qualifications required by paragraph (b) of this section, a flight termination system safety official shall have the following knowledge, experience and training:

(1) A degree in engineering. A candidate flight termination system safety official may substitute equivalent technical experience and education in lieu of a degree.

(2) Technical education, training, and experience in electronics, including command transmitters, antennas, and receivers/decoders.

(3) Technical education, training, or experience in ordnance handling, ordnance safety, and effectiveness of ordnance devices.

(4) Experience as an observer of a fully qualified flight termination system official for at least two launches.

(5) Experience as a flight termination system safety official, under the supervision of a qualified flight termination system safety official, for at least one launch.

(m) *Flight safety analyst role.* A launch operator shall designate a flight safety analyst for each launch. This person shall analyze whether a launch vehicle requires a flight termination system, evaluate flight safety data, establish flight safety hazard areas, prepare a flight safety plan in accordance with § 415.115 of this chapter, develop flight commit criteria and flight termination rules, establish and display flight safety limits, perform public safety analyses, and develop flight safety system crew training scenarios in coordination with the senior flight safety official.

(n) *Flight safety analyst qualifications.* In addition to the qualifications required by paragraph (b) of this section, a flight safety analyst shall have the following knowledge, experience, and training:

(1) A degree in engineering, mathematics, physics or other scientific discipline with equivalent mathematics and physics requirements.

(2) Knowledge of orbital mechanics and aerodynamics.

(3) Training on all components that are involved in the calculation and production of the range safety displays and the calculation of probability of impact and expected casualties. This training shall include the interrelationships and sensitivity of the results to changes in each of the components.

(4) Experience as an observer and assistant to a qualified flight safety analyst on all the preparations for at least one launch.

(5) Experience as a flight safety analyst under the supervision of a qualified flight safety analyst, on all the preparations for at least two launches.

§§ 417.332–417.400 [Reserved]

Subpart E—Ground Safety

§ 417.401 Scope.

This subpart contains public safety requirements that apply to launch processing and post-launch operations at a launch site in the United States. The ground safety requirements in this subpart apply to all activities performed by, or on behalf of, a launch operator at a launch site in the United States. A licensed launch site operator must satisfy the requirements of part 420 of this chapter. Launch processing and post-launch operations at a launch site outside the United States may be subject to the requirements of the governing jurisdiction.

§ 417.403 General.

(a) *Public safety.* A launch operator shall ensure that all hazard controls are in place to protect the public from any and all hazards associated with its launch processing at a launch site in the United States.

(b) *Ground safety analysis.* A launch operator shall perform and document a ground safety analysis in accordance with § 417.405.

(c) *Ground safety plan.* A launch operator shall implement the ground safety plan it submitted during the license application process according to § 415.117 of this chapter and in accordance with the launch plan requirements of § 417.111 and § 415.119 of this chapter. A launch operator shall ensure that its ground safety plan is readily available to the FAA, including any FAA safety inspector at the launch site, and to personnel involved in operations at the launch site that could endanger the public. A launch operator shall keep current its ground safety plan for each launch and shall submit any change to the FAA no later than 15 days before the change is implemented. A launch operator shall submit any change that is material to public health and safety to the FAA for approval as a license modification in accordance with § 415.73 of this chapter. Any change that involves the addition of a hazard that could affect the public or the elimination of any previously identified hazard control for a hazard that still exists constitutes a material change.

(d) *Local agreements.* A launch operator shall coordinate and perform launch processing and flight of a launch vehicle in accordance with any local agreements that ensure that the responsibilities and requirements in this part and § 420.57 of this chapter are met. When a launch operator uses the launch site of a licensed launch site operator, the launch operator shall ensure that its own operations are conducted in accordance with any agreements that the launch site operator has with local authorities and that form a basis for the launch site operator's license.

(e) *Launch operator's exclusive use of a launch site.* For a launch that is to be conducted from a launch site exclusive to its own use, a launch operator shall satisfy the requirements of this subpart and applicable requirements of part 420 of this chapter, including the requirements contained in §§ 420.31 through 420.37 and subpart D of part 420.

§ 417.405 Ground safety analysis.

(a) A launch operator shall perform a ground safety analysis for all its launch vehicle hardware and launch processing at a launch site in the United States. This analysis must identify each potential public hazard, any and all associated causes, and any and all hazard controls that a launch operator will implement to keep each hazard from reaching the public. A launch operator's ground safety analysis must demonstrate whether its launch vehicle hardware and launch processing create public hazards. A launch operator shall incorporate any launch site operator's hardware systems and operations into a ground safety analysis where these items are involved in ensuring public safety for the launch operator's launch vehicle and launch processing.

(b) A ground safety analysis must be prepared by a technically competent person who oversees and integrates the sub-analyses performed by engineers or other technical personnel who are the most knowledgeable of each ground system and operation and any associated hazards. This individual shall possess each of the following qualifications:

(1) An engineering or other similar technical degree.

(2) At least 30 hours of training in the discipline of system safety.

(3) At least ten years of technical work experience, with at least five of those years involved in launch vehicle ground operations that provided a broad-based familiarity with ground processing safety hazards and the precautions needed to prevent mishaps.

(4) A background in reviewing complex technical documentation.

(5) The communication skills necessary to translate complex technical documentation into clear explanations and figures and to produce a ground safety analysis report.

(c) A launch operator shall ensure that personnel performing a ground safety analysis or preparing a ground safety analysis report have the support of the launch operator's entire organization and that any supporting documentation is maintained and available upon request.

(d) A launch operator shall begin a ground safety analysis by identifying all the systems and operations to be analyzed. A launch operator shall define the extent of each system and operation being assessed to ensure there is no miscommunication as to what the hazards are, and who, in the launch operator's organization or other organization supporting the launch, is responsible for controlling those hazards. A launch operator shall ensure that the ground safety analysis accounts for each launch vehicle system and operation involved in launch processing, even if only to show that no public hazard exists.

(e) A ground safety analysis need not account for potential hazards of a component if the launch operator demonstrates that no hazard to the public exists at the system level. A ground safety analysis need not account for an operation's individual task or subtask level if the launch operator demonstrates that no hazard to the public exists at the operation level. For any hazard that is confined within the boundaries of a launch operator's facility not to be a hazard to the public, the launch operator must provide verifiable controls that ensure the public will not have access to the associated hazard area while the hazard exists.

(f) A launch operator shall identify all hazards of each launch vehicle system and launch processing operation in accordance with the following:

(1) System hazards shall include explosives and other ordnance, solid and liquid propellants, and toxic and radioactive materials. Other system hazards include, but are not limited to, asphyxiants, cryogens, and high pressure. System hazards generally exist even when no operation is occurring.

(2) Operation hazards to be identified derive from an unsafe condition created by a system or operating environment or an unsafe act.

(3) All hazards, both credible and non-credible, shall be identified. The probability of occurrence is not relevant with respect to identifying a hazard.

(4) The ground safety analysis must provide a rationale for any assertion that no hazard exists for a particular system or operation.

(g) A launch operator shall categorize all hazards identified in accordance with the following:

(1) *Public hazard.* A launch operator shall treat any hazard that extends beyond the launch location under the control of the launch operator as a public hazard. Public hazards include, but need not be limited to:

(i) Blast overpressure and fragmentation resulting from an explosion.

(ii) Fire and deflagration, including of hazardous materials such as radioactive material, beryllium, carbon fibers, and propellants. When assessing systems containing such materials, a launch operator shall assume that in the event of a fire, hazardous smoke will reach the public.

(iii) Any sudden release of a hazardous material into the air, water, or ground.

(iv) Inadvertent ignition of a propulsive launch vehicle payload, stage, or motor.

(2) *Launch location hazard.* A hazard that extends beyond individuals doing the work, but stays within the confines of the location under the control of the launch operator. The confines may be bounded by a wall or a fence line of a facility or launch complex, or by a fenced or unfenced boundary of an entire industrial complex or multi-user launch site. A launch location hazard may effect the public depending on public access controls. Launch location hazards that may effect the public include, but are not limited to, the hazards listed in paragraphs (g)(1)(i) through (iv) of this section and additional hazards in potentially unsafe locations accessible to the public such as:

(i) Unguarded electrical circuits or machinery.

(ii) Oxygen deficient environments.

(iii) Falling objects.

(iv) Potential falls into unguarded pits or from unguarded elevated work platforms.

(v) Sources of high ionizing and non-ionizing radiation such as x-rays, radio transmitters, and lasers.

(3) *Employee hazard.* A hazard only to individuals performing the launch operator's work and not a hazard to other people in the area. A launch operator is responsible for employee safety in accordance with other federal and local regulations. For any hazard determined to be an employee hazard, a launch operator's ground safety analysis must identify the hazard and demonstrate that there are no associated public safety issues.

(4) *Non-credible hazard.* A hazard for which any possible adverse effect on

people or property would be negligible and where the possibility of any adverse effect on people or property is remote. For any hazard determined to be non-credible, a launch operator's ground safety analysis must identify the hazard and demonstrate that it is non-credible.

(h) For each public hazard and launch location hazard, a ground safety analysis must identify all hazard causes. The analysis must account for conditions or acts or any chain of events that could result in a hazard. The analysis must account for the possible failure of any control or monitoring circuitry within hardware systems that could cause a hazard.

(i) A ground safety analysis must identify the controls to be implemented by a launch operator for each hazard cause identified in accordance with paragraph (h) of this section. A launch operator's hazard controls shall include, but need not be limited to the use of engineering controls for the containment of hazards within defined areas and the control of public access to those areas.

(j) All hazard controls selected by a launch operator must be verifiable in accordance with § 415.117(b)(3) of this chapter. If a hazard control is not verifiable, a launch operator may include it as an informational note on the hazard analysis form, if a verifiable control is also listed.

(k) A licensee shall ensure the continuing accuracy of its ground safety analysis in accordance with the requirements of this paragraph. A launch operator shall document the results of its ground safety analysis in a ground safety analysis report as required during the license application process in accordance with § 415.117 and appendix B to part 415 of this chapter. The analysis of ground systems and operations shall not end upon submission of a ground safety analysis report to the FAA during the license application process.

(1) A licensee shall ensure that any new or modified system or operation is analyzed for potential hazards that could effect the public. A licensee shall also ensure that each existing system and operation is subject to continual scrutiny and that the information in a ground safety analysis report is kept current.

(2) A licensee shall submit any ground safety analysis report update or change to the FAA as soon as the need for the change is identified and at least 30 days before any associated activity is to take place. Any change that involves the addition of a hazard that could effect the public or the elimination of any previously identified hazard control for a hazard that still exists, shall be submitted to the FAA for approval as a license modification.

§ 417.407 Hazard control implementation.

(a) *General.* A launch operator shall implement the hazard controls identified by its ground safety analysis. System hazard controls must be implemented in accordance with § 417.409. Safety clear zones for hazardous operations must be implemented in accordance with § 417.411. Hazard areas and controls for allowing any public access must be implemented in accordance with § 417.413. Hazard controls after launch or an attempt to launch must be implemented in accordance with § 417.415. Controls for propellant and explosive hazards shall be implemented in accordance with § 417.417.

(b) *Hazard control verification.* A launch operator shall implement a hazard tracking process to ensure that each hazard has a verifiable hazard control. Verification status shall remain ''open'' for an individual hazard control until the hazard control is verified to exist in a released drawing, report, procedure or similar document.

(c) *Hazard control configuration control.* A launch operator shall institute a configuration control process for safety critical hardware and procedural steps to ensure that verified hazard controls and their associated documentation cannot be changed without coordination with the launch safety director.

(d) *Inspections.* When a hazard exists, a launch operator shall conduct daily inspections of all related hardware, software, and facilities to ensure that all safety devices and other hazard controls are in place for that hazard, and that all hazardous and safety critical hardware and software is in working order and that no unsafe conditions exist.

(e) *Procedures.* Each launch processing operation involving a public hazard or a launch location hazard must be conducted in accordance with written procedures that incorporate the hazard controls identified by the launch operator's ground safety analysis and as required by this subpart. The launch operator's launch safety director must approve such procedures. A launch operator shall maintain an ''as-run'' copy of these procedures, which includes any changes and provides historical documentation of start and stop dates and times that the procedure was run and any observations made during the operation.

(f) *Hazardous materials.* A launch operator shall implement procedures for the receipt, storage, handling, use, and disposal of hazardous materials, including toxic substances and any sources of ionizing radiation. A launch operator shall implement procedures for responding to hazardous material emergencies and protecting the public in accordance with its emergency response plan submitted through the licensing process according to § 415.119(b) of this chapter. These procedures must include identification of each hazard and its effects, actions to be taken in response to release of a hazardous material, identification of protective gear and other safety equipment that must be available in order to respond to a release, evacuation and rescue procedures, chain of command, communication both on-site and off-site to surrounding communities and local authorities. A launch operator shall perform a toxic release hazard analysis for any launch processing performed at the launch site in accordance with appendix I of this part. A launch operator shall apply toxic plume modeling techniques in accordance with appendix I and ensure that notifications and evacuations are accomplished to protect the public from any potential toxic release.

§ 417.409 System hazard controls.

(a) *General.* For each system that presents a public hazard, a launch operator shall implement hazard controls as identified by its ground safety analysis and in accordance with the requirements of this section.

(1) A system must be no less than single fault tolerant to creating a public hazard unless other hazard control criteria are specified for the system by the requirements of this part, such as the requirements for structures and material handling equipment contained in paragraph (b) of this section. A system capable of creating a catastrophic public hazard, such as a liquid or solid stage inadvertently going propulsive or a release of a toxic substance that could reach the public, shall be no less than dual fault tolerant. Dual fault tolerance includes, but need not be limited to, switches, valves or similar components that prevent an unwanted transfer or release of energy or hazardous materials.

(2) Each hazard control used to provide fault tolerance must be independent from any other hazard control so that no single action or event can remove more than one inhibit. A launch operator must prevent inadvertent actuation of actuation devices such as switches and valves.

(3) If a safety device or other item must function in order to control a public safety hazard, at least two fully

redundant items shall be provided. No single action or event shall be capable of disabling both items.

(4) Any computing systems and software used to control a public hazard must satisfy the requirements of § 417.123 and appendix H of this part.

(b) *Structures and material handling equipment.* Any safety factor applied in the design of a structure or material handling equipment must account for static and dynamic loads, environmental stresses and expected wear. A launch operator shall inspect structures and material handling equipment to verify workmanship and proper operations and maintenance. A launch operator shall assess its structures and material handling equipment for potential single point failures that could endanger the public. Single point failures shall be eliminated or subject to specific inspection and testing that ensures proper operation. All single point failure welds must undergo both surface and volumetric inspection to verify no critical flaws. If, due to the geometry of a weld, a meaningful volumetric inspection cannot be performed, a launch operator shall implement other inspection techniques. In such a case, the launch operator shall demonstrate, clearly and convincingly, through the licensing process that its inspection processes accurately verifies the absence of any critical flaw.

(c) *Pressure vessels and pressurized systems.* A launch operator shall apply the following hazard controls to any flight or ground pressure vessel, component, or system that will be pressurized during launch processing and whose failure, during launch processing, could endanger the public:

(1) A pressure vessel, component, or system must be tested upon installation and before being placed into service, and periodically inspected to ensure that no critical flaw exists.

(2) Any safety factor applied in the design of a pressure vessel, component, or system must account for static and dynamic loads, environmental stresses and expected wear.

(3) Except for pressure relief and emergency venting, pressurized system flow-paths must be single fault tolerant to causing pressure ruptures and material releases that could endanger the public during launch processing.

(4) Pressure relief and emergency venting capability must be provided to protect against pressure ruptures that could endanger the public. Pressure relief devices shall be sized to provide the flow rate necessary to prevent a rupture in the event a pressure vessel is exposed to fire.

(d) *Electrical and mechanical systems.* A launch operator shall apply the following hazard controls to any electrical or mechanical system that could release electrical or mechanical energy that could endanger the public during launch processing:

(1) Electrical and mechanical systems must be single fault tolerant to providing or releasing electrical or mechanical energy that could endanger the public. This requirement includes systems that generate ionizing or non-ionizing radiation.

(2) Electrical systems and equipment used in areas where a flammable material may exist must be hermetically sealed, explosion proof, intrinsically safe, purged or otherwise designed so as not to provide an ignition source. A launch operator shall assess each electrical system as a possible source of thermal energy and ensure that the electrical system could not act as an ignition source.

(3) A launch operator shall prevent unintentionally conducted or radiated energy due to possible bent pins in a connector, a mismated connector, shorted wires, or unshielded wires within electrical power and signal circuits that interface with hazardous subsystems.

(e) *Propulsion systems.* A propulsion system must be dual fault tolerant to inadvertently becoming propulsive. Propulsion systems must be single fault tolerant to inadvertent mixing of fuel and oxidizer. Each material in a propulsion system must be compatible with any other material that it may come into contact with during launch processing. This includes any material used to assemble and clean the system. Different sized fittings shall be used to prevent connecting incompatible systems. Hazard controls applicable to propellants and explosives are provided in § 417.417.

(f) *Ordnance systems.* An ordnance system must be at least single fault tolerant to prevent inadvertent actuation if the public could be reached. Hazard controls applicable to ordnance are provided in § 417.417. In addition, an ordnance system must satisfy the following requirements:

(1) All ordnance and electrical connections shall be kept disconnected until final preparations for flight.

(2) An ordnance system must provide for safing and arming of all ordnance. An electrically initiated ordnance system must include ordnance initiation devices or arming devices, also referred to as safe and arm devices, that provide a removable and replaceable mechanical barrier or other positive means of interrupting power to each ordnance firing circuit to prevent inadvertent initiation of ordnance. A mechanical safe and arm device must have a safing pin that locks the mechanical barrier in a safe position. A mechanical actuated ordnance device must also have a safing pin that prevents mechanical movement within the device. Specific safing and arming requirements for a flight termination system are provided in § 417.313.

(3) An ordnance system must be protected from stray energy through grounding, bonding, or shielding.

(4) Any monitoring or test circuitry that interfaces with an ordnance system must be current limited to protect against inadvertent initiation of ordnance. Equipment used to measure bridgewire resistance on electro-explosive devices must be special purpose ordnance system instrumentation with features that limit current.

§ 417.411 Safety clear zones for hazardous operations.

(a) For each operation involving a potential launch location hazard or public hazard, a launch operator shall define a safety clear zone within which any potential adverse effects of the hazard will be confined. A launch operator may employ a risk analysis to define a safety clear zone if, through the licensing process, the launch operator demonstrates clearly and convincingly an equivalent level of safety. A launch operator's safety clear zones must satisfy the following:

(1) A launch operator shall establish a safety clear zone that accounts for the potential blast, fragment, fire or heat, toxic and other hazardous energy or material potential of the associated systems and operations.

(2) Any time a launch vehicle is in a launch commandable configuration, the flight safety system shall be fully operational, on internal power, with the associated safety clear zone in effect and cleared.

(3) A safety clear zone for a possible explosive event shall be based on the worst case possible event, regardless of the fault tolerance of the system.

(4) A safety clear zone for a possible toxic event shall be based on the worst case credible event. A launch operator shall have procedures in place, in a stand-by condition, so as to maintain public safety in the event toxic releases reach beyond the safety clear zone.

(5) A safety clear zone for a material handling operation shall be based on a worst case credible event for that operation, such as failure of a component in the lifting device while lifting a fueled spacecraft.

(b) A launch operator shall implement restrictions that prohibit public access to any safety clear zone during the hazardous operation. A safety clear zone may extend to areas beyond the launch location boundaries if local agreements provide for restricting public access to such areas and the launch operator verifies that the safety clear zone is clear of any public during the hazardous operation.

(c) A launch operator's procedures shall verify that the public is outside of a safety clear zone prior to the launch operator beginning the hazardous operation.

(d) A launch operator shall control a safety clear zone to ensure no public access during the associated operation. This may include the use of security guards and equipment, physical barriers, and warning signs and other types of warning devices.

§ 417.413 Hazard areas.

(a) *General.* For each hardware system that presents a public hazard or launch location hazard, a launch operator shall define a hazard area within which any adverse effects will be confined should an actuation or other hazardous event occur. Whenever a hazard is present, a launch operator shall prohibit public access to any hazard area unless the requirements for public access of paragraph (b) of this section are met.

(b) *Public access.* If visitors or other members of the public, such as individuals providing goods or services not related to the launch processing or flight of a launch vehicle, must have access to a launch operator's facility or launch location, a launch operator shall implement a process for authorizing public access on an individual basis. This process must ensure that each member of the public is briefed on all hazards within the facility and any related safety warnings, procedures, or rules that provide protection, or the launch operator shall ensure that each individual is accompanied at all times by a fully knowledgeable escort.

(c) *Hazard controls during public access.* A launch operator shall implement procedural controls that preclude any hazardous operation from taking place while members of the public have access to the launch location and that system hazard controls are in place that preclude initiation of a hazardous event. Hazard controls that preclude initiation of a hazardous event include, but need not be limited to, the following:

(1) Lockout devices or other restraints must be used on system actuation switches or other controls to eliminate the possibility of inadvertent actuation of a hazardous system.

(2) Ordnance systems must be physically disconnected from any power source, incorporate the use of safing plugs, or have safety devices in place that preclude inadvertent initiation. If the safety devices are electrically actuated, no activity involving the control circuitry for those safety devices shall be ongoing while the public has access to the hazard area. All safing pins on safe and arm devices and mechanically actuated devices must be installed. All explosive transfer lines, not protected by a safe and arm device or mechanically actuated device or equivalent, must be physically disconnected.

(3) When systems or tanks are loaded with hypergols or other toxic materials, the system or tank must be closed and verified to be leak-tight with two verifiable closures, such as a valve and a cap, to every external flow path or fitting. Such a system must also be in a steady-state condition. A launch operator shall also visually inspect a propellant system to check for potential leak sources and problems.

(4) Any pressurized system must not be above its maximum allowable working pressure or be in a dynamic state. If a pressurized system has valves that are electrically actuated, no activity involving this circuitry shall be ongoing while the public has access to the associated hazard area. Any launch vehicle system shall not be pressurized to more than 25% of its design burst pressure, when the public has access to the associated hazard area.

(5) Any sources of ionizing or non-ionizing radiation, such as, x-rays, nuclear power sources, high-energy radio transmitters and radar and lasers must not be present or must be verified to be inactive when the public has access to the associated hazard area.

(6) Any physical hazards must be guarded to prevent potential physical injury to any visiting member of the public. Physical hazards include, but need not be limited to potential falling objects, personnel falls from an elevated position, and protection from potentially hazardous vents, such as pressure relief discharge vents.

(7) Any safety device or safety critical system must be maintained and verified to be operating properly prior to permitting public access.

§ 417.415 Post-launch and post-flight-attempt hazard controls.

(a) A launch operator shall implement procedures for controlling hazards and returning the launch facility to a safe condition after a successful launch. Procedural hazard controls must include, but need not be limited to, provisions for extinguishing any fires and re-establishing full operational capability of all safety devices, barriers and platforms, and access control.

(b) A launch operator shall implement procedures for controlling hazards associated with a failed flight attempt where a solid or liquid launch vehicle engine start command was sent, but the launch vehicle did not liftoff. These procedures must include, but need not be limited to, the following:

(1) Maintaining and verifying that any flight termination system remains operational until it is verified that the launch vehicle does not represent a risk of inadvertent liftoff. If an ignition signal has been sent to a solid rocket motor, there must be a waiting period of no less than 30 minutes during which the flight termination system must remain armed and active. During this time flight termination system batteries must maintain sufficient voltage and current capacity for flight termination system operation and the flight termination system receivers must remain captured by the command control system transmitter's carrier signal.

(2) Assuring that the vehicle is in a safe configuration, including its propulsion and ordnance systems. The flight safety system crew shall have access to the vehicle status. Safety devices shall be re-established and any pressurized systems shall be brought down to safe pressure levels.

(3) Prohibiting launch complex entry until a pad safing team has performed all necessary safing tasks.

(c) A launch operator shall implement procedural controls for hazards associated with an unsuccessful flight where the launch vehicle has a land or water impact. These procedures must include, but need not be limited to the following:

(1) Provisions for extinguishing any fires.

(2) Provisions for evacuation and rescue of members of the public, to include modeling the dispersion and movement of any toxic plume, identification of areas at risk, and communication with local government authorities.

(3) Provisions to secure impact areas to ensure that all personnel are evacuated, that no unauthorized personnel enter, and to preserve evidence.

(4) Provisions for ensuring public safety from any hazardous debris, such as plans for recovery and salvage of launch vehicle debris and safe disposal of any hazardous materials.

§ 417.417 Propellants and explosives.

(a) A launch operator shall comply with the explosive safety criteria in 14 CFR part 420.

(b) A launch operator shall ensure compliance with the explosive site plan developed in accordance with 14 CFR part 420 by ensuring that:

(1) Only those explosive facilities and launch points addressed in the explosive site plan are used and only for their intended purpose.

(2) The total net explosive weight for each explosive hazard facility and launch point must not exceed the maximum net explosive weight limit indicated on the explosive site plan for each location.

(c) A launch operator shall implement procedures that ensure public safety for the receipt, storage, handling, inspection, test, and disposal of explosives.

(d) A launch operator shall implement procedural system controls to preclude inadvertent initiation of propellants and explosives. These controls shall include, but need not be limited to, the following:

(1) Ordnance systems must be protected from stray energy through methods of bonding, grounding, and shielding, and by controlling radio frequency radiation sources in a radio frequency radiation exclusion area. A launch operator shall determine the vulnerability of its electro-explosive devices and systems to radio frequency radiation and establish radio frequency radiation power limits or radio frequency radiation exclusion areas as required by the launch site operator or as needed to ensure safety.

(2) Ordnance safety devices, as described in § 417.409, must remain in place until the launch complex is cleared as part of the final launch countdown. No members of the public shall be allowed back onto the complex until all safety devices are re-established.

(3) Heat and spark or flame producing devices must not be allowed in an explosive or propellant facility without written approval and oversight, such as obtaining a hot work permit, from a launch operator's launch safety organization.

(4) Static producing materials must not be allowed in close proximity to solid or liquid propellants, electro-explosive devices or systems containing flammable liquids.

(5) Fire safety measures shall be used to preclude inadvertent initiation of propellants and explosives including, but not limited to, the elimination or reduction of flammable and combustible materials, elimination or reduction of ignition sources, fire and smoke detection systems, safe means of egress and timely fire suppression response.

(6) A facility used to store or process explosives must include lightning protection to prevent inadvertent initiation of propellants and explosives due to lightning.

(7) In the event of an emergency, a launch operator shall implement its emergency response plan, developed in accordance with § 415.119(b) of this chapter and updated in accordance with § 417.111, to provide for the control of any propellant or explosive hazards.

§§ 417.418–417.500 [Reserved]

Appendix A to Part 417—Methodologies for Determining Hazard Areas for Orbital Launch

A417.1 General

This appendix provides methodologies and equations for use in determining the hazard areas and public risk factors as part of the flight hazard area analyses required by § 417.225. A launch operator shall use the methodologies and equations provided in this appendix when performing the analyses unless a launch operator provides a clear and convincing demonstration that an alternative provides an equivalent level of safety.

A417.3 Blast Hazard Area

(a) *General.* A launch operator shall use the following equations and methodologies when determining a blast hazard area as required by § 417.225.

(b) *Input.* To determine the blast hazard area associated with any potential explosive hazard, a launch operator shall identify the weight and the TNT equivalency coefficient (C) of each explosive source for use as input to the analysis calculations.

(c) *Methodology.* For each explosive hazard, a launch operator shall calculate a blast hazard area for an overpressure of 3.0 pounds per square inch defined by a radius R_{op} around the location of the explosive source using the following equations:

$$R_{op} = 20.3 \cdot (NEW)^{1/3}$$

Where:

R_{op} is the over pressure distance in feet.
$NEW = W_E \cdot C$ (pounds).
W_E is the weight of the explosive in pounds.
C is the TNT equivalency coefficient of the propellant being evaluated. A launch operator shall identify the TNT equivalency of each propellant on its launch vehicle including any payload. TNT equivalency data for common liquid propellants is provided in tables A417–1. Table A417–2 provides factors for converting gallons of specified liquid propellants to pounds.

A417.5 Ship-Hit Contours in the Flight Hazard Area

(a) *General.* A launch operator shall use the equations and methodologies contained in this section when determining ship hazard areas, referred to as ship-hit contours, as required by § 417.225(g).

(b) *Input.* A launch operator's hazard area analysis must account for the following input data when determining ship-hit contours:

(1) The debris class mean impact points and standard deviations (sigma) of the impact dispersions for each simulated launch vehicle failure for increasing trajectory times (T) from liftoff until the instantaneous impact point reaches a downrange distance such that the ship hit probability becomes less than 1×10^{-5}. A launch operator shall determine debris impacts and dispersions in accordance with § 417.225(a)(3). The debris impact dispersions must account for the variance in ballistic coefficient for each debris class, winds, variance in velocity resulting from vehicle breakup, and tumble turn and guidance errors. When determining a ship-hit contour, the launch operator need not account for debris with a ballistic coefficient of less than three. A launch operator shall ensure that a ship-hit contour consists of curves that are smooth and continuous. This shall be accomplished by varying the time interval (Δt), between the trajectory times assessed such that each debris impact point location change, between time intervals, is less than one-half sigma of the downrange dispersion distance.

(2) The probability of failure of each launch vehicle stage and the probability of existence of each debris class which must account for break up through aerodynamic breakup or a flight termination action and the different debris that would result from each type of break up. Any planned debris impact, such as a stage or payload fairing impact, shall be accounted for as a debris class with a probability of existence equal to the probability of success for the planned debris impact.

(3) The size of the largest ship that could be located in the flight hazard area, or, where the ship size is unknown, a launch operator shall use a ship size of 600 feet long by 200 feet wide. A launch operator may use a ship size less than 600 feet long by 200 feet wide, if the launch operator demonstrates clearly and convincingly through the licensing process that its proposed ship size represents the largest ship that could be present in the flight hazard area.

(c) *Ship surveillance in the flight hazard area.* A launch operator shall use statistical ship density data to determine the need to survey ships in the flight hazard area during the launch countdown. A launch operator need not survey for ships if the launch operator demonstrates, using statistical ship density data, that the collective probability of hitting any ship is less than or equal to 1×10^{-5}. A launch operator shall determine whether ship surveillance in the flight hazard area is required for a launch in accordance with the following:

(1) A launch operator shall determine ship density for the flight hazard area based on the most recent statistical data from maritime reports, satellite analysis, or U.S. government information. The ship density for the flight hazard area must account for time of day and any other factors that might affect the ship density. The statistical ship density for the flight hazard area must be multiplied by a safety factor of 10 for use in the collective ship-hit probability analysis unless the

launch operator demonstrates the accuracy of its ship density data, clearly and convincingly through the licensing process, and accounts for the associated ship density error in the collective ship-hit probability analysis.

(2) A launch operator shall use the methodology contained in paragraph (d) of this section to determine a ship-hit contour for 10 ships where the probability of hitting any one of the 10 ships located on the contour is less than or equal to 1×10^{-5}.

(3) A launch operator shall compute the expected number of ships inside the 10-ship contour determined according to paragraph (c)(2) of this section by determining the total water surface area within the 10-ship contour and multiplying this area by the ship density determined according to paragraph (c)(1) of this section. If the resulting number of ships is less than 10, ship surveillance in the flight hazard area is not required and the launch operator need only determine the ship hazard area for notice to mariners according to paragraph (e) of this section. If the resulting number of ships is equal to or greater than 10, ship surveillance in the flight hazard area is required and the launch operator shall determine the ship-hit contours according to paragraph (d) of this section.

(d) *Methodology for determining ship-hit contours in the flight hazard area.* A launch operator shall use the methodology contained in this paragraph to determine ship-hit contours as required by § 417.225. Each ship-hit contour shall be designated by a number N_S, which equals the number of ships (1 through 10) represented by the contour. Each contour must define the area where if N_S ships were located on the contour, the probability of debris impacting a ship during launch vehicle flight would be less than or equal to 1×10^{-5}. A launch operator shall determine a ship-hit contour for each NS by evaluating each $T + \Delta t$ trajectory time step and computing the ship-hit probability for N_S ship(s) assumed to be located at grid points of increasing crossrange distance from the nominal instantaneous impact point trace in accordance with the following:

(1) A launch operator shall establish a grid of ship location points separated by no more than 1000 feet in both the downrange direction and the crossrange direction. Figure A417–1 illustrates a grid of ship location points and sample debris impact points for three debris classes labeled 1, 2, and 3. To determine an N_S ship-hit contour, a launch operator shall compute the hit probability for N_S ships located at each ship location grid point due to each potential debris impact for each trajectory time T, and sum the hit probabilities for each ship location grid point over all trajectory times, assuming a probability of each impact occurring that is applicable to each trajectory time.

(2) If the debris dispersion for a debris class has equal values for left and right crossrange, or uprange and down range, the launch operator need only perform calculations in one elliptical quadrant and then may assume that the ship-hit probability is symmetrical in the other quadrant and multiply the probability result for the calculated quadrant by the number of symmetrical quadrants.

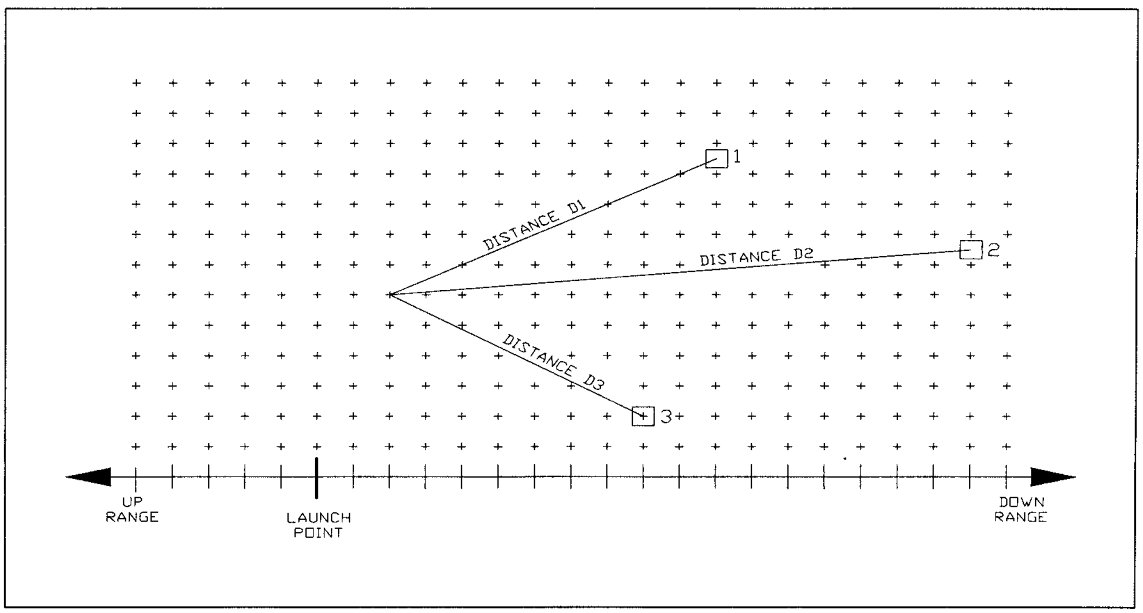


Figure A417-1, Illustration of a Grid of Ship Location Points and Debris Impact Points.

(3) Figure A417–2 illustrates a ship location point, labeled ''1'', with four debris impact points, surrounded by their dispersions, for a given trajectory time of T. A launch operator shall use the following sequence of steps to evaluate each such ship location point when determining a ship-hit contour:

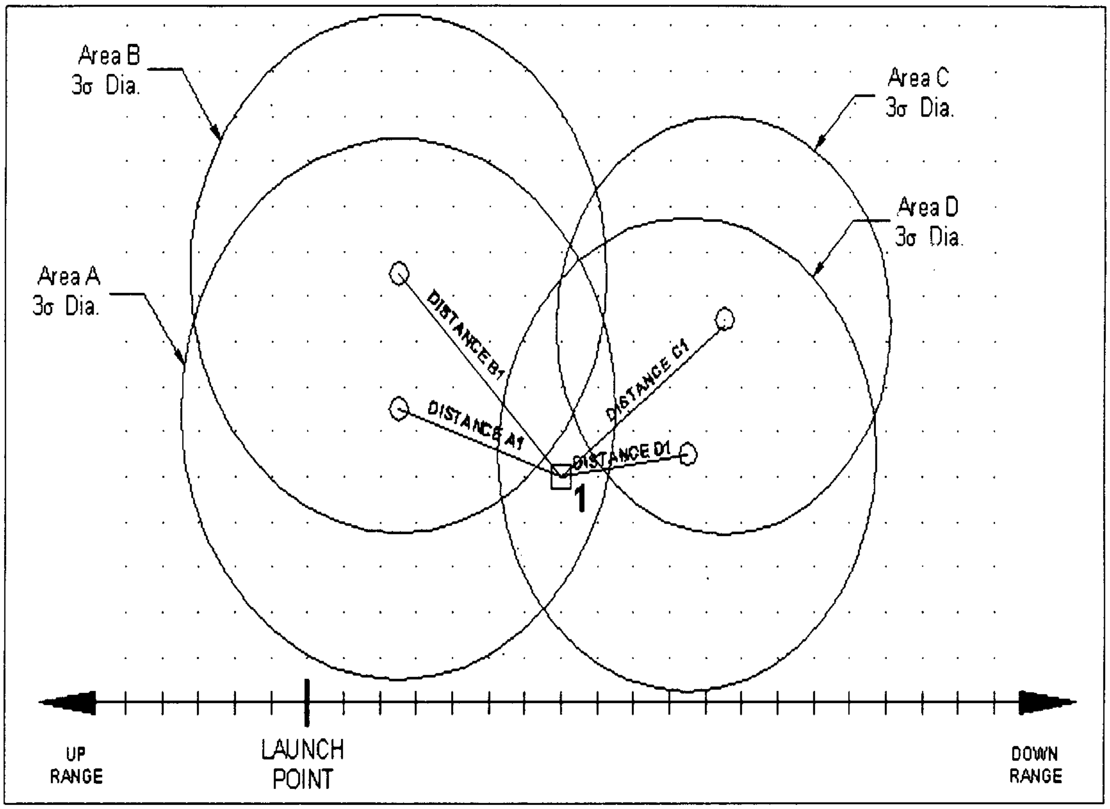


Figure A417-2, Illustration of a Ship Location Point and Debris Impact Dispersions

(i) For each ship location point that is within the four-sigma distribution of any debris impact, compute the probability of hitting a ship, P_S, for each debris class using the following equations:

$$F_D = \frac{e^{-\frac{1}{2}\left(\frac{D}{\sigma}\right)^2}}{2\pi\sigma^2}$$

Where:

F_D is the probability density function.

D is the distance from the mean impact point of the debris class to the ship location grid point during the time interval (see Figure A417–2). It is only necessary to evaluate those debris impacts for which

$$\frac{D}{\sigma}$$

is less than 4.

σ is the standard deviation of the debris class impact dispersion.

$$P_{c(A,B,---N)} = P_{E(A,B,---N)} \times F_{D(A,B,---N)} \times A$$

Where:

$P_{C\,(A,B,---N)}$ is the conditional hit probability for each debris class (A,B,---N) during the Δt time interval.

$P_{E\,(A,B,---N)}$ is the probability of existence for each debris class (A,B,---N) during the Δt time interval.

$F_{D\,(A,B,---N)}$ is the probability density function determined for each debris class (A,B,---N) during the Δt time interval.

A is the total area of the N_S ships.

$$P_{GT} = P_F\left[1-\left(1-P_{CA}\right)^{NA}\left(1-P_{CB}\right)^{NB}\ldots\left(1-P_{CN}\right)^{NN}\right]$$

Where:

$N_{A,B,--N}$ are the number of debris pieces in each debris class.

P_F is the probability of failure during the Δt time interval.

P_{GT} is the ship-hit probability for each ship location grid point at each Δt time interval.

P_{GT} is then summed over all time intervals to obtain P_S:

$$P_s = \sum P_{GT}$$

Where:

P_S is the total ship-hit probability for the ship location grid point, summed over all time intervals and for all debris pieces.

P_{GT} is the ship-hit probability for each ship location grid point, for a specific trajectory time interval for which a failure probability is established.

(ii) Compute P_S as a running total for each grid point from lift-off until the P_S, computed in step (i) for a grid point located directly on the nominal instantaneous impact point trace, is equal to or less than 1×100^{-5} and all debris impact points reach a distance greater than four sigma from this impact point. This downrange distance represents the end of the N_s ship-hit contour.

(iii) Once a launch operator determines the end of a ship-hit contour on the nominal instantaneous impact point trace, the launch operator shall define the crossrange distance for each time step along the nominal trajectory where the ship-hit probability is equal to or less than 1×10^{-5}. A launch operator may refine this distance by linearly interpolating the log of P_S between ship location grid points, such as $\log_{10}(P_S)$. The ship-hit contour for N_S ships shall be determined by drawing straight line segments connecting the ship location points where P_S is equal to or less than 1×10^{-5}. The area enclosed by the ship-hit contour represents the ship hazard area for N_S ships.

(iv) Repeat steps (i) through (iii) to determine each N_S ship-hit contour as required by § 417.225(g)(1).

(e) *Ship hazard area for notice to mariners.* Regardless of whether ship surveillance is required according to paragraph (c) of this section, a launch operator shall determine a ship hazard area for providing notice to mariners as the ship-hit contour for 10 ships determined according to paragraph (d) of this section. A launch operator shall ensure that a notice of this ship hazard area is disseminated in accordance with § 417.121(e).

A417.7 Individual Casualty Contour

(a) *General.* For land overflight, an individual casualty contour must encompass the area where the individual casualty probability (P_C) criteria of 1×10^{-6} established in § 417.107(b) would be exceeded if one person were assumed to be in the open, inside the contour, during launch vehicle flight. A launch operator shall use the equations and methodologies provided in this section to define an individual casualty contour as required by § 417.225(d).

(b) *Input.* A launch operator shall use the following input data when determining an individual casualty contour:

(1) The standard deviation of the impact debris dispersions for each debris class produced by all launch vehicle failures assessed every t + Δt interval from launch until the individual risk, P_C, associated with that launch becomes less than 1×10^{-6}. A launch operator shall determine debris impacts and dispersions in accordance with § 417.225(a)(3). When determining an individual casualty contour, a launch operator need not account for debris with a ballistic coefficient of less than three. A launch operator shall ensure that an individual casualty contour consists of curves that are smooth and continuous. This shall be accomplished by varying the time interval (Δt) between the trajectory times assessed such that each debris impact point location change, between time intervals, is less than one-half sigma of the downrange dispersion distance.

(2) The probability of failure of each launch vehicle stage.

(3) The probability of existence of each debris class.

(c) *Methodology for determining individual risk for debris impacts.* A launch operator shall use the following methodology for determining individual risk and an individual casualty contour:

(1) A launch operator shall establish a grid of personnel location points that are no more than 1000 feet apart in the downrange direction and no more than 1000 feet apart in the crossrange direction (see figure A417–1). For each t + Δt time interval starting at first stage ignition, the probability of casualty (P_C) shall be computed assuming a person is in the open and is located at grid points of increasing crossrange distance from the nominal instantaneous impact point trace. As instantaneous impact point rates increase and the debris impact points become more dispersed, the delta time shall decrease inversely as a function of the instantaneous impact point rate. At each grid point, the probability of each type of vehicle failure will be evaluated according to its probability of occurrence at that time point. A launch operator shall compute P_C for each grid point and sum the probabilities of casualty for that grid point over all flight times for grid points of increasing crossrange distance from the nominal instantaneous impact point trace until PC is less than or equal to 1×10^{-6} for all debris classes where the grid point is within the four-sigma impact dispersion of the debris class using the following equation:

$$P_C = \sum_{t=0}^{t=T} P_{G_{(t)}}$$

Where:

P_C is the total probability of casualty, summed over all times and for all pieces, for one person in the open located at a grid point.

$P_{G(t)}$ is the probability of casualty for one person in the open located at a grid point for all launch vehicle failures during a specific time interval.

(2) A launch operator shall use the methodology in paragraph (d) of this section to compute $P_{G_{(t)}}$ for inert debris impact locations.

(3) A launch operator shall use the methodology in paragraph (e) of this section to compute $P_{G_{(t)}}$ for explosive or other types of hazardous debris for which the size of the casualty area is greater than 0.5 sigma of the debris impact dispersion. If the casualty area is less than or equal to 0.5 sigma of the debris impact dispersion, the launch operator may use the methodology in paragraph (d) of this section to compute $P_{G_{(t)}}$.

(4) When several hazardous debris pieces exist in a debris class, a launch operator shall use a standard statistical procedure for combining the probability of casualty for each debris piece to determine the probability of casualty for the mean debris piece of the debris class in accordance with the following equation:

$$p_c(\text{class}) = 1 - \left[1 - p(\text{component})\right]^{N_c P_E}$$

Where:

P_C is the probability of casualty for debris class C.

N_C is the number of components in debris class C.

P_E is the probability that the hazard will exist upon impact for each component in debris class C (for example the probability that an explosive debris piece will explode upon impact.

(5) A launch operator shall use the methodology and equations in this paragraph when combining probability of casualty of different debris classes or debris types such as inert and explosive hazards, to obtain the total probability of casualty. Additionally, if hazards such as explosive components do not produced an explosive hazard area (propellant pieces have a probability of explosion as a function of the impact velocity), their impact would be treated in the same manner as inert pieces and the following equation still applies, since the number of pieces would explode on impact and the number that would not always sum to N_C. If, for example, there are N_C components in the Cth hazardous debris class and P_E is the probability that the hazard will exists upon impact for each component, the probability of casualty for one or more classes may be approximated using the following equations:

$$P_{G_{(t)}} = P_F \cdot \left[1 - \left(1 - P_{C_A}\right)^{N_A P_E}\left(1 - P_{C_B}\right)^{N_B P_E} \ldots \left(1 - P_{C_N}\right)^{N_N P_E}\right]$$

Where:

$N_{A,B-N}$ are the number of debris pieces in each debris class.

P_F is the probability of vehicle failure during the time interval Δt, at time t,

P_E is the probability of existence for each debris class during the Δt,

$P_{G(t)}$ is the probability of casualty for each grid point for a time interval.

$$P_C = \sum_{t=0}^{t=T} P_{G(t)}$$

(6) A launch operator shall compute P_C as a running total summation of each time interval and for each grid point from launch until the total probability of casualty for a grid point located on the nominal instantaneous impact point is less than 1×10^{-6} and any further debris impacts are greater than four sigma from this grid point. The resulting downrange position represents the end of the individual casualty contour.

(7) Once the end of the individual casualty contour is determined, a launch operator shall determine all cross range distances to the grid points at which the probability of casualty is less than 1×10^{-6}. A launch operator may refine this distance by linearly interpolating the log of P_C between grid points (i.e. $\log_{10}$)P_C. The individual casualty contour shall be determined by drawing strait line segments connecting the personal location grid points where P_C is equal to or less than 1×10^{-6}. The area enclosed by the individual casualty contour represents the individual casualty hazard area.

(d) *Methodology for determining individual risk for inert debris impacts.* A launch operator shall use the following sequence of calculations to determine the probability of casualty for each personnel location grid point for an inert debris impact for an inert debris class as required in paragraph (c)(2) of this section:

$$F_D = \frac{e^{-\frac{1}{2}\left(\frac{D}{\sigma}\right)^2}}{2\pi\sigma^2}$$

Where:

D is the distance from the impact point of the debris class to the grid point (see figure A417–2). Calculations are only necessary for cases in which

$$\frac{D}{\sigma}$$

is less than 4.0.

σ is the circular normal standard deviation of the debris class impact dispersion. F_D is the probability density function.

$$P_{C_{A,B,-N}} = F_D \cdot A_C$$

Where:

A_C is the casualty area for the debris class.

P_C is the probability of casualty for the inert debris class (A, B–N).

(e) *Methodology for determining individual risk for explosive or other hazardous debris impacts.* This paragraph contains the methodology for computing the probability of casualty for explosive or other debris impacts with hazard areas larger than 0.5-sigma of the debris impact dispersion. Inert debris generally has a casualty area that is small in comparison to its dispersion (less than 0.5-sigma of the impact dispersion) and therefore applying the probability density function, F_D, to the entire casualty area in a single calculation, as required in paragraph (d) of this section, provides for a valid approximation of the hit probability. Explosive and other hazardous debris have much larger casualty areas where, in order to obtain a valid approximation of the hit probability, an integration process is required. The integration process varies depending on the type of situation that exists for the hazardous area with respect to the location of the mean point of impact and its dispersion. These situations produce various integration limits and integration ranges, which are described in paragraph (f) of this section. Figure A417–3 provides an example, using overpressure as the hazard, of the integration process for a single failure-response mode, time point, and debris class that shall be evaluated in accordance with the following:

(1) Figure A417–3 shows a circular overpressure casualty area of radius R_{op} about a grid point where a person is assumed to be located. R_{op} represents the casualty area radius for each debris class, and includes the piece of debris that produces the greatest radius. The probability of casualty is therefore the probability of having an impact of the hazardous explosive debris occurring such that the circle defined by R_{op} covers a grid point location. The probability of impact inside circle R_{op} shall be determined by integrating the hazardous debris' impact density function over the area of circle R_{op}. The circular area of radius R_{max} about the mean point of impact (MPI) represents the limit of all possible impacts, and represents a debris dispersion of four-sigma (4σ). If d is the distance between the MPI and the grid point, the integration must be performed under the density-function surface between the range limits of (d-R_{op}) and (d+ R_{op}), and within the lateral bounds of the hazardous overpressure circle. Because of the assumed circular nature of the impact density functions about their respective MPIs, the integration is performed by slicing the hazardous overpressure circle into n truncated annular sections (or truncated slices) centered at the mean point of impact. One such slice is illustrated in figure A417–3.

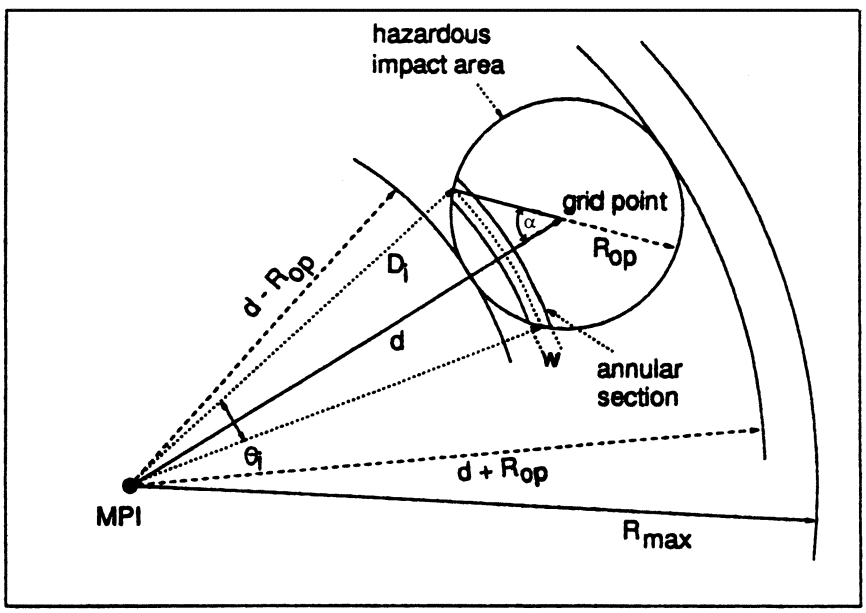


Figure A417-3

(2) If D_i represents the distance from the MPI to the middle arc of the i^{th} truncated slice and w is the width of the slice, the volume under the slice is found by integrating the density function between the range limits of ($D_i - w/2$) and ($D_i+w/2$), and between the angular limits bounded by the sides of the angle θ_i. The sum for all volumes between the limits of ($d - R_{op}$) and ($d+R_{op}$) gives the probability of casualty at the grid point for one hazardous area, in one debris class, for one failure-response mode, and, if applicable, one failure time interval. If n is sufficiently large so that w is sufficiently small, a good approximation for the probability of impact in the i^{th}-truncated slice is:

$$p_i = w \cdot \theta \cdot D_i \cdot F\left(D_i\right)$$

Where:

$F(D_i)$ is the density function value at distance D_i from the MPI.

$w\ \theta_i\ D_i$ is the approximate area of the truncated slice.

Slice width w depends on the relative magnitudes of R_{max} and ($d+R_{op}$).

(3) A second approach must be used if the circularized explosive hazard area about the grid point encompasses the MPI as depicted in figure A417–4.

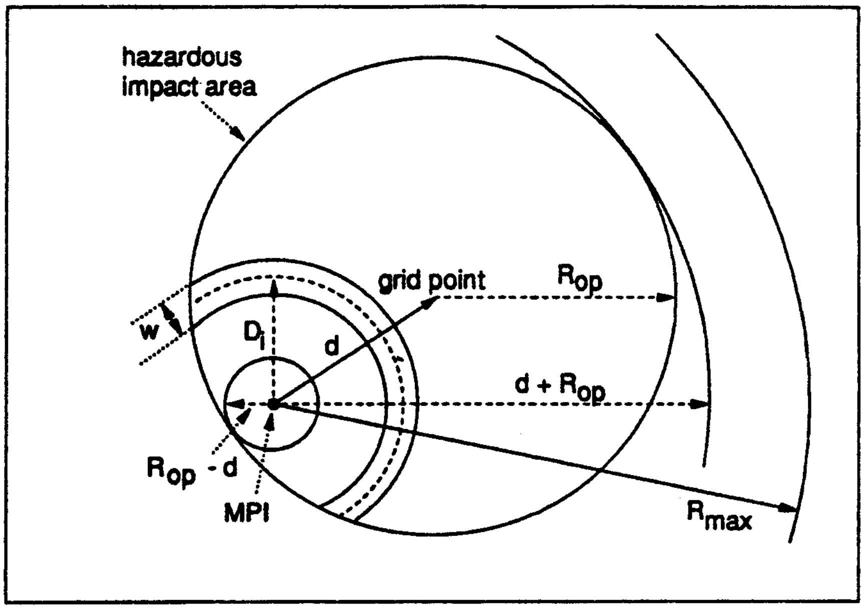


Figure A417-4

Where:

The circular area of radius R_{max} about the MPI represents the limit of all impacts, which is four sigma of the impact dispersion.

d is the distance between the MPI and grid point.

D_i is the distance from the MPI to the middle of the i^{th}-truncated slice.

w is the slice width.

(4) For the case illustrated by figure A417–4, $(R_{op} - d)$ is less than R_{max} and the impact density function is first integrated over the small circular area of radius $(R_{op} - d)$ centered at the MPI, to find the probability of impacting inside this circle. The remainder of the hazardous impact area is sliced into n truncated annular regions, and the impact probability for each slice found by integrating the density function between the range and angular limits of the slice. The probability of casualty at a grid point for explosive or other hazardous debris impacts shall be determined in accordance with the following:

$$p_G = p_0 + \sum_{i=1}^{n} p_i$$

Where:

ρ_0 is the probability of impacting in the circular area of radius $(R_{op} - d)$ centered at the MPI. ρ_0 is determined by integrating ''n'' probability circles to obtain the probability of casualty for the circle with radius of $(R_{op} - d)$,

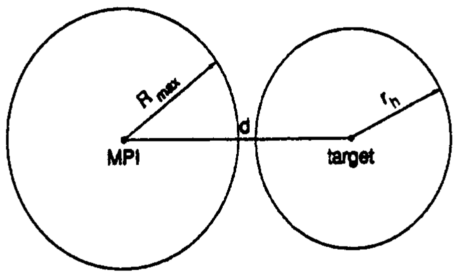
$$p_0 = \sum_{1}^{n} A_i \cdot F(D_i).$$

ρ_i is the probability of the i^{th} slice. ρ_i is computed by integrating slices of width (w) from $(R_{op} - d)$ to Rop or R_{max}, whichever is smallest,

$$p_i = w \cdot \theta_i \cdot D_i \cdot F(D_i).$$

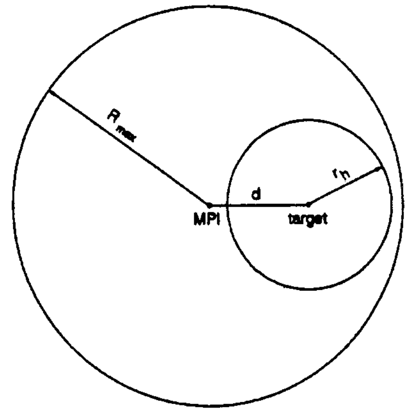
(5) The selected slice width (w) and limits of integration shall be as defined for each situation discussed in paragraph (f) of this section.

(f) *Geometric relationships (situations) in the integration process for determining individual risk.* In computing the probability that a person located at a grid point will be subjected to a hazard with a hazard radius r_h, six geometric situations arise, depending on the relative magnitudes of r_h, R_{max}, and d. These situations are illustrated in figures A417–5 through A417–10, and are referred to as situations 1 through 6. The 6 situations result in a variance in ring widths, integration step size, and integration limits used in computing the impact probabilities in the m+1 concentric circles about the grid point. This results in variations in R_{max}, r_h, and d. The term ''circle R_{max}'' or ''circle r_h'' means the circle having a radius of R_{max} or r_h. The circle R_{max} is always centered at the MPI while circles r_h are always centered at the grid point being investigated where a person is assumed to be located. As indicated previously, R_{max} is equal to a four-sigma debris impact dispersion.



Situation (1)

Figure A417-5



Situation (2)

Figure A417-6

(1) *Situation (1).* The circles R_{max} and r_h do not overlap ($d \geq R_{max} + r_h$), as illustrated in figure A417–5. For this situation the probability of impact in circle r_h is zero and no further integration is necessary. $P_C = 0$.

(2) *Situation (2).* The circle R_{max} contains all of circle r_h ($R_{max} \geq d + r_h$), and r_h does not contain the MPI ($r_h \leq d$), as illustrated in figure A417–6. Situation 2 doesn't have an initial inner circle and the integration limits are $d - r_h$ (lower) to $d + r_h$. (Upper). A launch operator's integration process shall incorporate the following:

(i) Compute slice width (w) by:

$$w = \frac{\text{upper limit} - \text{lower limit}}{N} = \frac{2r_h}{100}$$

Where N=100 is arbitrary in this case; N shall be selected so that w is ≥ 10% of σ or the delta integration angle of the target circle is ≥ 10°. Since integration is over π radians, the minimum N is 18.

(ii) Set $\rho_t = 0$. Start the integration by establishing the radius to the midpoint of the first slice w as

$$\frac{w}{2};$$

and the resulting radius becomes:

$$R_s = d - r_h + \frac{w}{2}; n = 1;$$

(iii) Compute F_D by:

$$F_D = \frac{e^{-\frac{1}{2}\left(\frac{D}{\sigma}\right)^2}}{2\pi\sigma^2}$$

Where:

$D = R_S$

σ is the circular normal standard deviation of the debris class impact dispersion of the impacting debris.

F_D is the probability density function.

(iv) Compute (θ using the Law of Cosines:

$$\frac{\theta}{2} = \cos^{-1}\left[\frac{R_S^2 + d^2 - r_h^2}{2R_s d}\right]$$

Where:

d is the distance from the impact point of the debris class to the grid point (see figure A417–2).

r_h is the hazard radius.

(v) Compute the probability of casualty for a slice by:

$$P_i = w \cdot \theta \cdot R_{S_i} \cdot F(R_{Si})$$

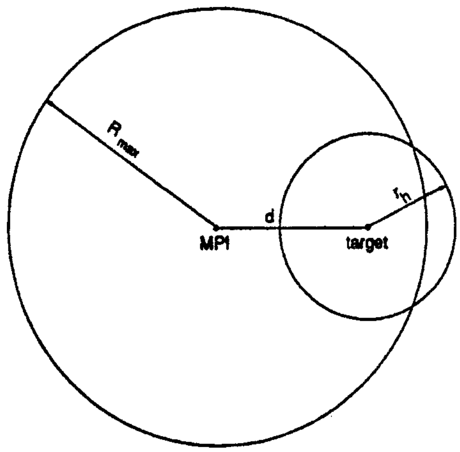
$$P_{C_{A,B,-N}} = P_E \cdot P_i + P_{C_{A,B,-N}}$$

Where:

P_E is the probability of existence for each debris class.

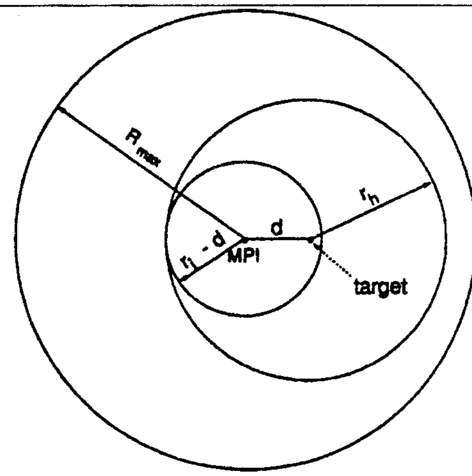
P_C is the probability of casualty for each debris class (A, B---N)

(vi) Integrate over the range of n by incrementing n to n +1 and R_S to R_S + w, and repeating steps (iii) through (v) until n = N.



Situation (3)

Figure 417-7



Situation (4)

Figure 417-8

(3) *Situation (3).* The circle R_{max} does not contain all of circle r_h ($R_{max}<d+r_h$), and r_h does not contain the MPI ($r_h \leq d$), as illustrated in figure A417–7. Situation 3 doesn't have an initial inner circle and the integration limits are $d-r_h$ (lower) to R_{max} (upper).

(i) Compute slice width (w) by:

$$w = \frac{\text{upper limit} - \text{lower limit}}{N} = \frac{R_{max} + r_h - d}{100}$$

Where N=100 is arbitrary in this case; N shall be selected so that w is ≥ 10% of σ or the delta integration angle of the target circle is ≥ 10°. Since integration is over π radians, the minimum N is 18.

(ii) Set $p_t = 0$. Start the integration by establishing the radius to the midpoint of the first slice w as

$$\frac{w}{2};$$

and the resulting radius (see figure A417–3) becomes:

$$R_s = d - r_h + \frac{w}{2}; n = 1;$$

(iii) Compute F_D by:

$$F_D = \frac{e^{-\frac{1}{2}\left(\frac{D}{\sigma}\right)^2}}{2\pi\sigma^2}$$

Where:

$D = R_S$.

σ is the circular normal standard deviation of the debris class impact dispersion of the impacting debris.

F_D is the probability density function.

(iv) Compute θ using the Law of Cosines:

$$\frac{\theta}{2} = \cos^{-1}\left[\frac{R_S^2 + d^2 - r_h^2}{2R_s d}\right]$$

Where:

d is the distance from the impact point of the debris class to the grid point (see figure A417–2).

r_h is the hazard radius.

(v) Compute the probability of casualty for a slice by:

$$P_i = w \cdot \theta \cdot R_{S_i} \cdot F(R_{Si})$$

$$P_{C_{A,B,-N}} = P_E \cdot P_i + P_{C_{A,B,-N}}$$

Where:

P_E is the probability of existence for each debris class.

P_C is the probability of casualty for each debris class (A, B---N)

(vi) Integrate over the range of n by incrementing n to n +1 and R_S to R_S + w, and repeating steps (iii) through (v) until n = N.

(4) *Situation (4).* The circle R_{max} contains all of circle r_h ($R_{max} \geq d+r_h$), and r_h contains the MPI ($r_h>d$), as illustrated in figure A417–8. The impact probability for the small circle of radius ($r_h - d$) is found by closed-form computation and added to the sum obtained from a step-by-step integration across the remainder of circle r_h. Situation 4 has an initial inner circle of radius $r_h - d$ and the integration limits are $r_h - d$ (lower) to r_h+d (upper).

(i) Compute slice width (w) by:

$$w = \frac{\text{upper limit} - \text{lower limit}}{N} = \frac{2d}{100}$$

Where N=100 is arbitrary in the case; N shall be selected so that w is ≥10% of σ or the delta integration angle of the target circle is ≥10°. Since integration is over π radians, the minimum N is 18.

(ii) Set $P_t = 0$. Start the integration by establishing the radius to the midpoint of the first slice w as

$$\frac{w}{2};$$

and the resulting radius (see figure A417–3) becomes:

$$R_s = r_h + \frac{w}{2} - d; n = 1;$$

(iii) Compute F_D by:

$$F_D = \frac{e^{-\frac{1}{2}\left(\frac{D}{\sigma}\right)^2}}{2\pi\sigma^2}$$

Where:

$D = R_S$.

σ is the circular normal standard deviation of the debris class impact dispersion of the impacting debris;

F_D is the probability density function.

(iv) Compute θ using the Law of Cosines

$$\frac{\theta}{2} = \cos^{-1}\left[\frac{R_S^2 + d^2 - r_h^2}{2R_S d}\right]$$

Where:

d is the distance from the impact point of the debris class to the grid point (see figure A417–2).

r_h is the hazard radius.

(v) Compute the probability of casualty for a slice by:

$$P_i = w \cdot \theta \cdot R_{S_i} \cdot F(R_{S_i})$$

$$P_{C_{A,B,-N}} = P_E \cdot P_i + P_{C_{A,B,-N}}$$

Where:

P_E is the probability of existence for each debris class.

P_C is the probability of casualty for each debris class (A, B---N)

(vi) Integrate over the range of n by incrementing n to n+1 and R_S to R_S + w, and repeating steps (iii) through (v) until n = N.

(vii) Compute the casualty probability for the inner circle by subdividing the inner circle with radius $r_h - d$ into 10 circles for integration by:

$$w_r = \frac{r_h - d}{10};$$

(viii) With $r_I = w_r$ and $A_L = 0$, repeat the following for 10 summations:

$$A_i = \pi r_i^2$$

$$D = r_i - \frac{w_r}{2}$$

$$F_D = \frac{e^{-\frac{1}{2}\left(\frac{D}{\sigma}\right)^2}}{2\pi\sigma^2};$$

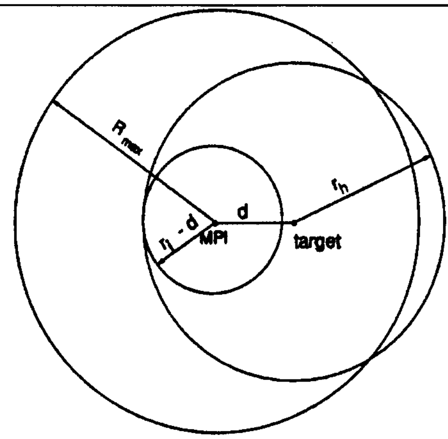
$$A = A_I - A_L$$

$$p_i = A \cdot F(R_{S_i})$$

$$A_L = A_I$$

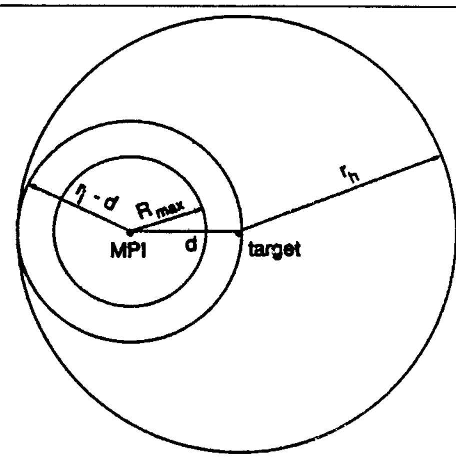
$$r_I = r_I + w_r$$

$$P_{C_{A,B,-N}} = P_E \cdot p_i + P_{C_{A,B,-N}}$$



Situation (5)

Figure A417-9



Situation (6)

Figure A417-10

(5) *Situation (5).* The circle R_{max} does not contain all of circle r_h ($R_{max}<d+r_h$) circle r_h contains the MPI ($r_h>d$), and $R_{max}>r_h - d$, as illustrated in figure A417–9. The impact probability for the small circle of radius ($r_h - d$) is found by closed-form computation and added to the sum obtained from a step-by-step integration across the remainder of circle r_h that is inside circle R_{max}. Situation 5 has an initial inner circle of radius $r_h - d$ and the integration limits are $r_h - d$ (lower) to R_{max} (upper).

(i) Compute slice width (w) by:

$$w = \frac{\text{upper limit} - \text{lower limit}}{N} = \frac{R_{max} + d - r_h}{100}$$

Where N=100 is arbitrary in this case; N shall be selected so that w is ≥ 10% of σ or the delta integration angle of the target circle is ≥ 10°. Since integration is over π radians, the minimum N is 18.

(ii) Set p_t=0. Start the integration by establishing the radius to the midpoint of the first slice w as

$$\frac{w}{2};$$

and the resulting radius (see figure A417–3) becomes:

$$R_s = r_h + \frac{w}{2} - d; n = 1;$$

(iii) Compute F_D by:

$$F_D = \frac{e^{-\frac{1}{2}\left(\frac{D}{\sigma}\right)^2}}{2\pi\sigma^2}$$

Where:

$D=R_S$.

σ is the circular normal standard deviation of the debris class impact dispersion of the impacting debris;

F_D is the probability density function.

(iv) Compute θ using the Law of Cosines:

$$\frac{\theta}{2} = \cos^{-1}\left[\frac{R_S^2 + d^2 - r_h^2}{2R_s d}\right]$$

Where:

d is the distance from the impact point of the debris class to the grid point (see figure A417–2).

r_h is the hazard radius.

(v) Compute the probability of casualty for a slice by:

$$P_i = w \cdot \theta \cdot R_{S_i} \cdot F\left(R_{S_i}\right)$$

$$P_{C_{A,B,-N}} = P_E \cdot p_i + P_{C_{A,B,-N}}$$

Where:

P_E is the probability of existence for each debris class.

P_C is the probability of casualty for each debris class (A, B—N)

(vi) Integrate over the range of n by incrementing n to n+1 and R_S to R_S + w, and repeating steps (iii) through (v) until n = N.

(vii) Compute the casualty probability for the inner circle by subdividing the inner circle with radius $r_h - d$ into 10 circles for integration by:

$$w_r = \frac{r_h - d}{10}$$

(viii) With $r_I = w_r$ and $A_L = 0$, repeat the following for 10 summations:

$$A_i = \pi r_i^2$$

$$D = r_i - \frac{w_r}{2}$$

$$F_D = \frac{e^{-\frac{1}{2}\left(\frac{D}{\sigma}\right)^2}}{2\pi\sigma^2};$$

$$A = A_I - A_L$$

$$p_i = A \cdot F\left(R_{S_i}\right)$$

$$A_L = A_I$$

$$r_I = r_I + w_r$$

$$P_{C_{A,B,-N}} = P_E \times p_i + P_{C_{A,B,-N}}$$

(6) *Situation (6).* The circle R_{max} is contained inside r_h, as illustrated in figure A417–10. The impact probability for the small circle of radius R_{max} is one and no integration is necessary.

$$P_i = 1.$$

$$P_{C_{A,B,-N}} = P_E \cdot P_i + P_{C_{A,B,-N}}$$

TABLE A417–1.—LIQUID PROPELLANT EXPLOSIVE EQUIVALENTS

Propellant combinations	TNT equivalents
LO_2/LH_2	The larger of $8W^{2/3}$ or 14% of W. Where W is the weight of LO2/LH2.
LO_2/LH_2 + LO_2/RP–1	Sum of (20% for LO2/RP–1) the larger of $8W^{2/3}$ or 14% of W. Where W is the weight of LO_2/LH_2.
LO_2/RP–1	20% of W up to 500,000 pounds + 10% of W over 500,000 pounds. Where W is the weight of LO_2/RP–1.
N_2O_4/N_2H_4 (or UDMH or UDMH/N_2H_4 Mixture)	10% of W_2. Where W is the weight of the propellant.

TABLE A417–2.—PROPELLANT HAZARD AND COMPATIBILITY GROUPINGS AND FACTORS TO BE USED WHEN CONVERTING GALLONS OF PROPELLANT INTO POUNDS

Propellant	Hazard group	Compatibility group	Pounds/gallon	°F
Hydrogen Peroxide	II	A	11.6	68
Hydrazine	III	C	8.4	68
Liquid Hydrogen	III	C	0.59	−423
Liquid Oxygen	II	A	9.5	−297
Nitrogen Tetroxide	I	A	12.1	68
RP–1	I	C	6.8	68
UDMH	III	C	6.6	68
UDHM/Hydrazine	III	C	7.5	68

Appendix B to Part 417—Methodology for Performing Debris Risk Analysis

B417.1 General

A launch operator's debris risk analysis required by § 417.227 must be in accordance with the analysis constraints contained in § 417.227 and shall be performed using the equations and methodologies for calculating expected casualty (E_C) contained in this appendix unless, through the licensing process, the launch operator provides a clear and convincing demonstration that an alternate method provides an equivalent level of safety. A launch operator shall compute the total E_C due to debris as the sum of the E_C due to all planned debris impacts determined according to B417.3 and the E_C due to potential launch vehicle failure along the normal flight path, hereafter referred to as overflight E_C, determined in accordance with B417.5. For a launch vehicle that uses a flight termination system, the total E_C due to debris must also account for risk to populations outside the flight control lines in accordance with to B417.7.

B417.3 Planned Impact E_C

(a) *General.* A launch operator shall use the equations and methodologies contained in this section for calculating E_C for planned debris impacts.

(b) *Input for computing planned impact E_C.* A launch operator shall identify the input parameters in this paragraph for computing the E_C for planned debris impacts:

(1) The nominal impact location of each planned debris fragment and the standard deviation (sigma) of the impact dispersion distances from the nominal impact point each of the uprange, downrange, left crossrange, and right crossrange directions. A launch operator shall determine debris impacts and dispersions in accordance with § 417.227(b)(5).

(2) The probability of success of each debris impact, that is, one minus the probability of the launch vehicle failing prior to each debris jettison. The probability of success used for the impact of a planned debris fragment must account for all stages that burn prior to jettison of that debris fragment.

(3) The effective casualty area for each planned impacting debris fragment.

(4) The location and population density of each population center to be evaluated.

(c) *Methodology for computing planned impact E_C.* A launch operator shall compute the E_C for each population center within the five-sigma dispersion of the nominal impact point for each fragment of impacting debris planned as part of normal flight using the equations and steps in this paragraph:

(1) Compute the following for each population center within the five-sigma dispersion of each planned impact of a debris fragment:

$$P_i = [1.0 - P_f] \cdot P_p$$

$$P_p = \frac{A_p}{2\pi\sigma_x\sigma_y} \cdot \left(\exp - \frac{1}{2}\left(\left(\frac{x}{\sigma_x}\right)^2 + \left(\frac{y}{\sigma_y}\right)^2 \right) \right)$$

Where:

P_i is the probability of the planned debris fragment impacting the population center that has area A_p.

P_f is the failure probability of the launch vehicle prior to the stage or other planned impacting debris jettison.

P_p is the probability of impacting inside the population center with area A_p, assuming a successful flight.

A_p is the area of the population center.

σ_y is the crossrange standard diviation of the planned impact dispersion for each planned debris fragment.

σ_x is the downrange standard deviation of the planned impact dispersion for each planned debris fragment.

x and y are the downrange and crossrange distances between the nominal impact point location and the location of the centroid of the population center for each planned debris fragment.

(2) For each immpacting debris fragment, compute E_C for all population centers within the five-sigma dispersion using the following:

$$E_C = \sum P_i \cdot A_C \cdot P_d$$

Where:

P_i is the probability of a planned debris fragment impacting the population center with population density P_d.

A_C is the effective casualty area for the planned impacting debris fragment.

P_d is the population density of each population center.

(3) Sum all E_C values for all planned impacts to compute the total planned debris impact E_C.

B417.5 Methodology for Computing Overflight E_C

(a) *General.* A launch operator shall use the equations and methodologies contained in this section for calculating overflight E_C.

(b) *Input.* A launch operator shall identify the following input parameters:

(1) The nominal launch vehicle trajectory instantaneous impact points as a function of trajectory time and the standard deviation of the normal trajectory impact point dispersion in the crossrange direction for each trajectory time. A launch operator shall use the trajectory data determined in accordance with § 417.205 for an orbital launch or C417.3 of appendix C of this part for the launch of a suborbital rocket.

(2) The failure probability of each launch vehicle stage and the overall launch vehicle failure probability determined in accordance with § 417.227(b)(6).

(3) The effective casualty area for each impacting debris fragment associated with a launch vehicle failure as a function of trajectory time determined in accordance with the debris analysis required by § 417.209.

(c) *Methodology for computing overflight E_C.* A launch operator shall determine overflight E_C using the nominal instantaneous impact point data determined by the trajectory analysis performed in accordance with § 417.205(c) for an orbital launch or appendix C of this part for a suborbital launch for each trajectory time, and the following methodology:

(1) Start at liftoff, trajectory time (T)=0.

(2) Increase the distance along the nominal trajectory by one trajectory time interval (ΔT) to T+ΔT. Form a sector by drawing lines perpendicular to the nominal instantaneous impact point trace that intersect the impact point positions at both T and T+ΔT.

(3) Identify all population centers that are contained or partially contained within the sector and that have a left crossrange or right crossrange distance from the nominal instantaneous impact point that is less than or equal to five-sigma of the crossrange trajectory dispersion. If no population centers are identified repeat step (2). For each population center identified calculate the crossrange component of the probability of impact (P_y) using the following:

$$P_y = \frac{1}{\sqrt{2\pi}} \cdot \frac{\Delta y}{\sigma_y} \cdot e^{-\frac{1}{2}\left[\frac{y}{\sigma_y}\right]^2}$$

Where:

y is the crossrange distance from the nominal instantaneous impact point trace for the trajectory time being evaluated to the middle of the population center.

σ_y is the crossrange standard deviation for the trajectory time being evaluated.

Δy is the crossrange width of the population center for the trajectory time interval being evaluated. For computational purposes, Δy must not exceed one half the value of σ_y. If so, Δy shall be broken into equal parts with each part less than one half of the value of σy. P_y of each part must then be computed and summed to obtain the entire P_y.

(4) Calculate the probability of impact (P_i) for the overflight of each population center as follows:

$$P_i = P_f \cdot \left[\frac{T_D}{T_B}\right] \cdot P_y$$

Where:

P_f is the launch vehicle failure rate for the trajectory time interval being evaluated. A launch operator shall apply the failure rate for the launch vehicle stage that will be thrusting during the trajectory time interval being evaluated (if that specific failure rate is known) or the launch operator shall use the launch vehicle failure rate for the entire flight.

T_D is dwell time of the instantaneous impact point over the population center during the trajectory time interval being evaluated, assuming the launch vehicle flies a normal trajectory over the centroid of the population center. In each case T_D must be less than or equal to ΔT.

T_B is the burn time. If a launch operator uses a stage failure rate for P_f, T_B must be the burn time for that stage. If the launch operator uses the launch vehicle failure rate for the entire flight for P_f, T_B must equal the total launch vehicle burn time for all stages.

The ratio of T_D over T_B is the downrange component of the probability of impact for the population center being evaluated.

(5) For the current trajectory time, calculate E_C for each population center using the following:

$$E_C = \sum P_i \cdot A_C \cdot P_d$$

Where:

P_i is the probability of impacting the population center with population density P_d.

A_C is the sum total effective casualty area that accounts for all impacting debris fragment associated with a launch vehicle failure for the current trajectory time.

P_d is the population density of each population center.

The product of $A_C \cdot P_d$ shall be limited to no greater than the total population of the population center being evaluated.

(6) Repeat steps (2) through (5) for all trajectory time intervals until orbit or impact of the final stage is achieved. Sum all E_C values for all population centers and for all trajectory time intervals to determine the total overflight E_C.

B417.7 E_C for Populations Outside Flight Control Lines

(a) *General.* For a launch vehicle that uses a flight termination system, a launch operator shall use the equations and methodologies contained in this section to identify any populations outside the flight control lines in the area surrounding the launch point that could be exposed to significant risk due to impacting launch vehicle debris. The risk to such populations must be accounted for in the launch operator's debris risk analysis in accordance with § 417.227(b)(11).

(b) *Populations outside the flight control lines.* To determine if a debris risk analysis is required for populations outside the flight control lines, a launch operator shall compare population densities in sectors about the launch point to the population limits shown in figures B417.7–1 through B417.7–4 for the launch operator's launch vehicle type. Launch vehicle types are defined in paragraph (c) of this section. The launch operator shall determine the population densities in each sector based on the most current census data and projections for the date and time of flight.

(c) *Population limits.* Figures B417–1 through B417–4 and their accompanying tables identify population sectors around a launch point and the population limits for each sector as a function of the size of the launch vehicle and whether it is a new or mature launch vehicle. A launch operator shall use the population limits for a mature launch vehicle if its launch vehicle has flown more than 30 times and the launch operator demonstrates that the total vehicle failure rate is less than 10%. Otherwise, the launch operator shall use the population limits for a new launch vehicle. A launch operator shall use the population limits for a large launch vehicle if its launch vehicle is capable of lifting an 18,500-pound payload to a 100-nautical mile orbit or larger. Otherwise, a launch operator shall use the population limits for a medium or small launch vehicle. A launch operator shall determine the population limits that apply to its analysis in accordance with the following:

(1) *For a large mature launch vehicle.* A launch operator shall use the sector population limits labeled in figure B417–1.

(2) *For a medium or small mature launch vehicle.* A launch operator shall use the sector population limits in figure B417–2.

(3) *For a large new launch vehicle.* A launch operator shall use the sector population limits in figures B417–3.

(4) *For a medium or small new launch vehicle.* A launch operator shall use the sector population limits in figures B417–4.

(5) If a medium or small launch vehicle uses solid rocket motors in any stage other than the first stage, the tables for a large launch vehicle must be used.

(6) If a large launch vehicle uses solid rocket motors in any stage other than the first stage, it must be evaluated on a case by case basis.

(d) *Methodology for screening populations outside flight control lines.* A launch operator shall use the populations determined in accordance with paragraph (b) of this section and the sector population limits determined in accordance with paragraph (c) of this section to identify any populations outside flight control lines for which debris risk analysis must be performed. The launch operator shall screen the populations in each sector identified in figures B417–1 through B417–4 in accordance with the following:

(1) The launch operator shall compare the population in each sector with the population limit for each sector as determined according to paragraphs (b) and (c) of this section. If the population in a sector exceeds the population limit for that sector, the launch operator shall perform a debris risk analysis for that sector in accordance with paragraph (e) of this section.

(2) For all sectors with a population that is less than the limit, the launch operator shall determine the total population ratio by summing the ratios of the population to the population limit for all sectors. If the sum of population ratios for all sectors is greater than 1.0, the launch operator shall perform a debris risk analysis for a sufficient number of sectors to reduce the sum of population ratios of the remaining sectors to less than 1.0.

(e) *Debris risk analysis for populations outside flight control lines.* A launch operator shall perform an analysis to determine E_C for each population sector requiring a debris risk analysis as determined according to paragraph (d) of this section. The launch operator shall demonstrate the validity of such an analysis on a case-by-case basis through the licensing process. The launch operator's analysis must be in accordance with the following:

(1) The analysis must account for:

(i) All launch vehicle failure response modes and their probability of occurrence.

(ii) Potential launch vehicle failures beginning at liftoff and for each nominal trajectory time at intervals of no greater than two seconds.

(iii) The effects of intact launch vehicle impacts and potential launch vehicle breakup resulting from vehicle turns that exceed structural limits, and in accordance with the probability of their occurrence.

(iv) For launch vehicle breakup, the analysis must account for all debris impact locations and debris dispersion. The debris dispersion must account for inadvertent separation destruct system time delays, variances in impacts caused by winds, differences in debris ballistic coefficient, drag uncertainties, and breakup imported velocities.

(v) The probability density function for each debris class and for each launch vehicle failure response mode.

(vi) The inert and explosive debris effects on casualty area. For inert debris fragments the analysis must account for the effects of bounce, splatter, and slide.

(vii) The population density for each population center located within each sector being evaluated.

(viii) For each population center within the sector, the analysis must account for the probabilities of casualty from all debris, for all failure times, and all launch vehicle failure responses.

(2) Beginning at liftoff, trajectory time = 0, and for each nominal trajectory time, at intervals of no greater than two seconds, the launch operator shall compute E_C for each population center within each sector being evaluated and for each potential debris impact. The potential debris impacts must include potential launch vehicle intact impact and the impact of debris fragments resulting from breakup. The launch operator shall use the following equation:

$$E_C = P_i \cdot A_C \cdot P_d \cdot P_{FSS}$$

Where:

P_i is the probability of the debris being evaluated impacting within the population center being evaluated for the trajectory time being evaluated.

A_C is the effective casualty area for the impacting debris.

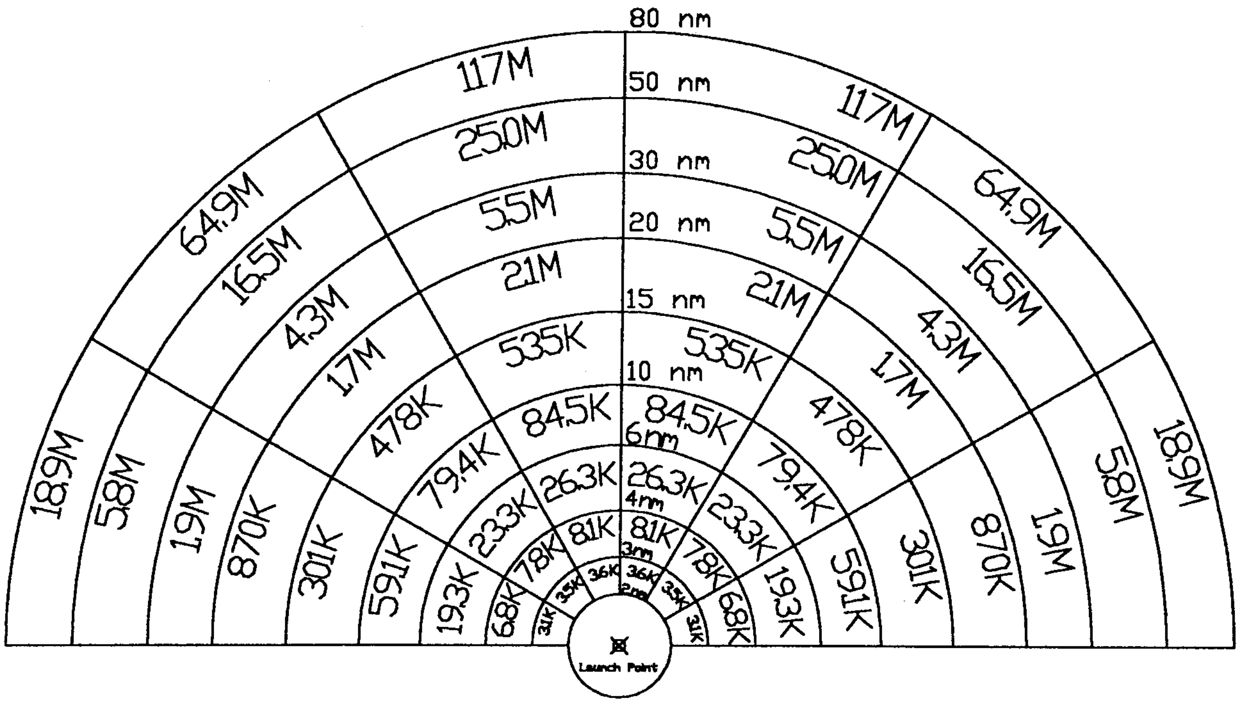
P_d is the population density of the population center being evaluated located within the sector.

P_{FSS} is the probability of failure of the launch operator's flight safety system. A launch operator may use 0.002 as the flight safety system probability of failure if the flight safety system is in compliance with the flight safety system requirements of subpart D of this part. For an alternate flight safety system approved in accordance with § 417.107(a)(3), the launch operator shall demonstrate the validity of the probability of failure on a case-by-case basis through the licensing process.

(3) The launch operator shall sum the E_C values for each potential debris impact, for each population center within a population sector being evaluated, and for each trajectory time and include this sum in the total E_C due to debris for the launch.

BILLING CODE 4910–13–P

Figure B417.7-1, Population Limits for Large Mature Launch Vehicles

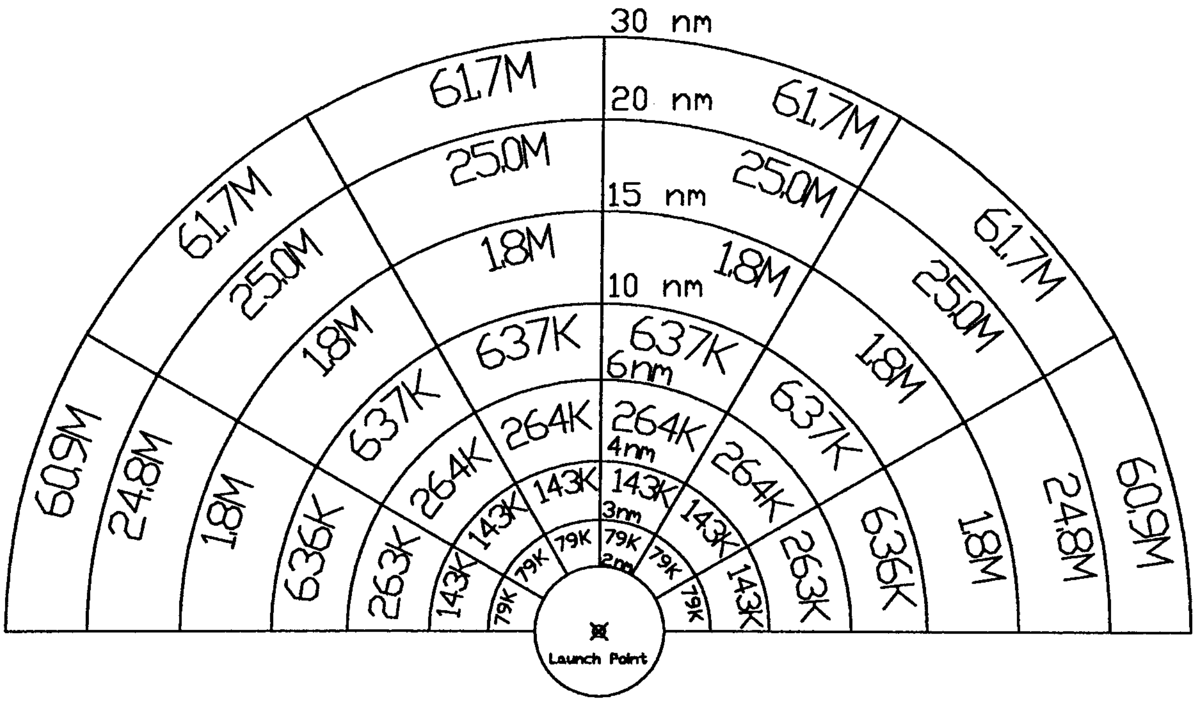


Numbers in sectors are given in terms of maximum number of people per sector.

Note: Each sector encompasses 30° of azimuth uprange of the launch point. The accompanying table contains the population limits for each sector.

Sector		Population Limits		
		Azimuth Angle from Uprange		
Range (nm)	Area (nm^2)	0° - 30°	30° - 60°	60° - 90°
2 – 3	1.309	3,556	3,478	3,111
3 – 4	1.833	8,084	7,770	6,775
4 – 6	5.236	26,340	23,320	19,320
6 – 10	16.76	84,530	79,370	59,140
10 – 15	32.72	535,300	477,800	300,800
15 – 20	45.81	2,135,000	1,744,000	870,300
20 – 30	130.9	5,531,000	4,290,000	1,926,000
30 – 50	418.9	25,010,000	16,500,000	5,757,000
50 – 80	1021	116,700,000	64,940,000	18,910,000

Figure B417.7-2, Population Limits for Medium Mature Launch Vehicles

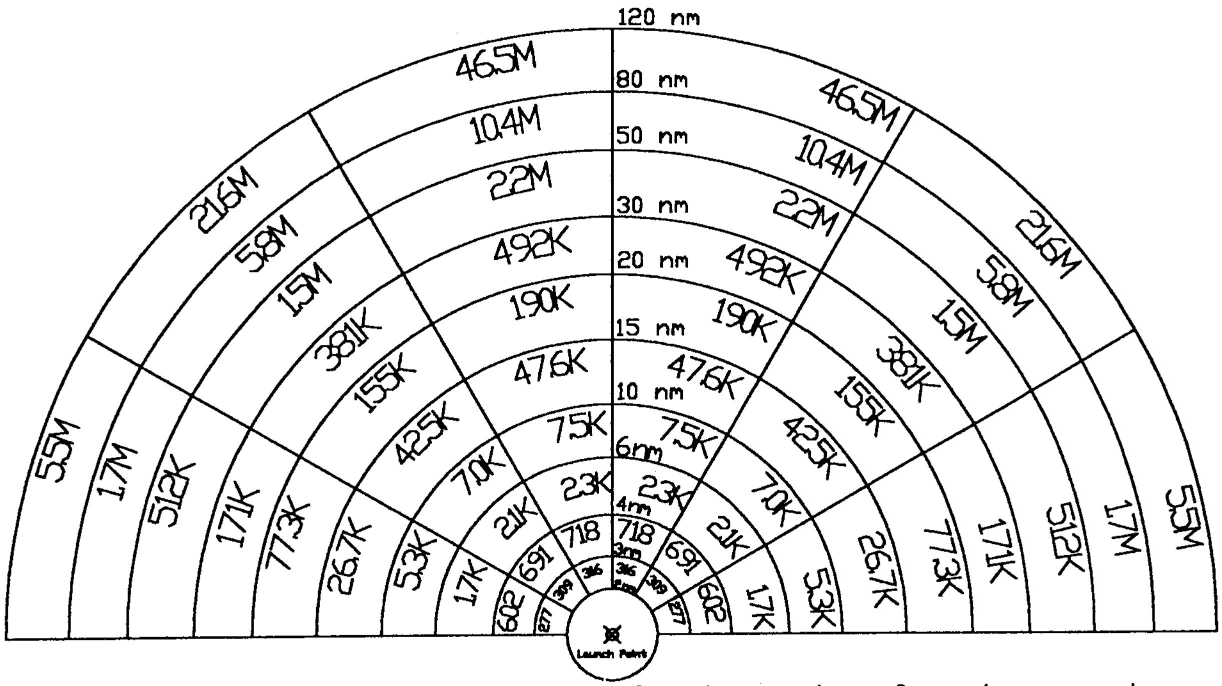


Numbers in sectors are given in terms of maximum number of people per sector.

Note: Each sector encompasses 30° of azimuth uprange of the launch point. The accompanying table contains the population limits for each sector.

Sector		Population Limits		
		Azimuth Angle from Uprange		
Range (nm)	Area (nm^2)	0° - 30°	30° - 60°	60° - 90°
2 – 3	1.309	78,930	78,930	78,740
3 – 4	1.833	143,000	143,000	142,800
4 – 6	5.236	263,500	263,500	263,200
6 – 10	16.76	636,900	636,900	636,100
10 – 15	32.72	1,815,000	1,813,000	1,812,000
15 – 20	45.81	25,030,000	25,020,000	24,770,000
20 – 30	130.9	61,730,000	61,690,000	60,900,000

Figure B417.7-3, Population Limits for Large New Launch Vehicles

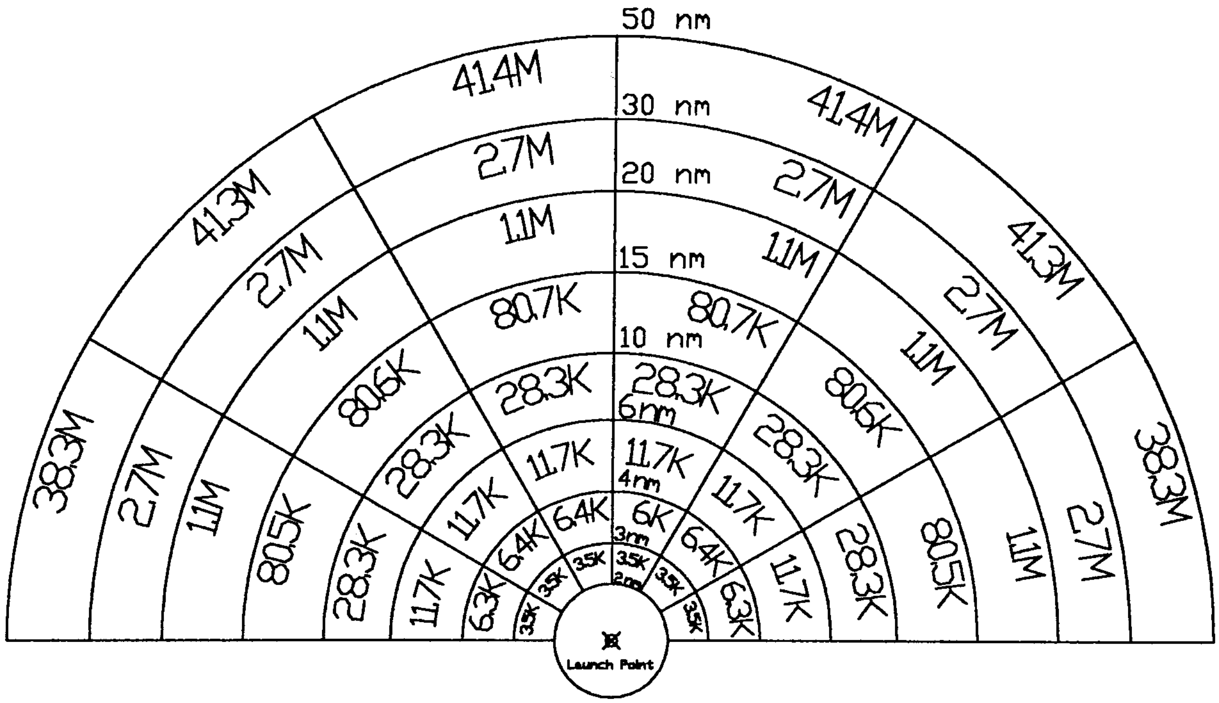


Numbers in sectors are given in terms of maximum number of people per sector.

Note: Each sector encompasses 30° of azimuth uprange of the launch point. The accompanying table contains the population limits for each sector.

Sector		Population Limits		
		Azimuth Angle from Uprange		
Range (nm)	Area (nm^2)	0° - 30°	30° - 60°	60° - 90°
2 – 3	1.309	316	309	277
3 – 4	1.833	718	691	602
4 – 6	5.236	2,342	2,073	1,718
6 – 10	16.76	7,513	7,047	5,258
10 – 15	32.72	47,570	42,460	26,740
15 – 20	45.81	189,800	155,000	77,340
20 – 30	130.9	491,600	381,400	171,200
30 – 50	418.9	2,223,000	1,467,000	511,800
50 – 80	1021	10,370,000	5,770,000	1,681,000
80 – 120	2094	46,530,000	21,630,000	5,495,000

Figure B417.4, Population Limits for Medium New Launch Vehicles



Numbers in sectors are given in terms of maximum number of people per sector.

Note: Each sector encompasses 30° of azimuth uprange of the launch point. The accompanying table contains the population limits for each sector.

Sector		Population Limits		
		Azimuth Angle from Uprange		
Range (nm)	Area (nm^2)	0° - 30°	30° - 60°	60° - 90°
2 – 3	1.309	3,508	3,508	3,500
3 – 4	1.833	6,357	6,357	6,345
4 – 6	5.236	11,710	11,710	11,700
6 – 10	16.76	28,300	28,300	28,260
10 – 15	32.72	80,650	80,580	80,520
15 – 20	45.81	1,112,000	1,112,000	1,101,000
20 – 30	130.9	2,743,000	2,741,000	2,706,000
30 – 50	418.9	41,410,000	41,290,000	38,310,000

B417.9 Alternative Debris Risk Analysis

(a) A launch operator may elect to simplify a debris risk analysis by making conservative assumptions that would lead to an overestimation of the total E_C due to debris. The intent of such an analysis would be to show that the overestimated E_C does not exceed the public safety criteria required by § 417.107(b). Such an analysis must be approved by the FAA during the licensing process. In addition to the analysis products required by § 417.227, a launch operator shall submit the following with respect to an alternative analysis:

(1) Identification of all assumptions made and explanation of how they relate to the debris risk analysis defined in B417.3, B417.5, and B417.7 of this appendix.

(2) Demonstration of how each assumption leads to overestimation of the total E_C due to debris.

(b) The following are examples of simplifications to the debris risk analysis that may be acceptable for a specific launch scenario:

(1) When flying over a remote area with limited population density, it may suffice to assume that P_i has a value of 1.0 for all population centers being evaluated.

(2) When computing overflight E_C, a launch operator may choose to analyze a worst case flight trajectory within the five-sigma corridor.

(3) A launch operator may choose to combine population centers and assume a

worst case population density for the combined area.

(4) A launch operator may choose to assume a worst case population density for the entire local launch area.

(5) A launch operator may choose to assume a worst case effective casualty area.

(c) A launch operator may employ an alternative analytical approach if the launch operator demonstrates, clearly and convincingly through the licensing process, that the proposed alternative provides an equivalent level of safety. The following requirements apply to any such alternative:

(1) The launch operator must demonstrate that any changes in inputs and assumptions are reasonable, based on accurate data, and statistically valid.

(2) A launch operator shall use the equations for calculating collective debris expected casualty required in this appendix.

(3) Use of risk analysis models such as those used at federal launch ranges in conjunction with validated input data, Monte Carlo simulation approaches, and refined (that is, higher fidelity) population data may constitute acceptable tools in support of a launch operator's alternative analysis.

(4) A launch operator may perform a sheltering analysis as a means of refining expected casualty calculations if the launch operator demonstrates that the analysis is reasonable, based on accurate data, and statistically valid. Rather than assuming that all people are in the open, a sheltering analysis accounts for populations that would be within a structure that may or may not provide the people some protection during the flight of a launch vehicle. Any sheltering analysis must account for any debris that will collapse or penetrate a structure and the increased casualty area that would result from such an event.

Appendix C to Part 417—Flight Safety Analysis for an Unguided Suborbital Rocket Flown With a Wind Weighting Safety System and Hazard Areas for Planned Impacts for All Launches

C417.1 General

This appendix contains methodologies for performing the flight safety analysis required for the launch of an unguided suborbital rocket flown with a wind weighting safety system. A launch operator shall perform a flight safety analysis to determine the launch parameters and conditions under which an unguided suborbital rocket may be flown using a wind weighting safety system in accordance with § 417.235. The results of this analysis must show that any adverse effects resulting from flight will be contained within controlled operational areas and any flight hardware or payload impacts will occur within planned impact areas. The flight safety analysis must demonstrate compliance with the safety criteria and operational requirements for the launch of an unguided suborbital rocket contained in § 417.125. A launch operator shall ensure that the flight safety analysis for an unguided suborbital rocket is conducted in accordance with the methodologies provided in this appendix unless the launch operator demonstrates, through the licensing process, that an alternate method provides an equivalent level of safety.

C417.3 Trajectory Analysis

(a) *General.* A launch operator shall perform a trajectory analysis for the flight of an unguided suborbital rocket to determine the launch vehicle's nominal trajectory, nominal drag impact points, and potential three-sigma dispersions about each nominal drag impact point.

(b) *Definitions.* A launch operator shall employ the following definitions when determining an unguided suborbital rocket's trajectory and drag impact points:

(1) *Drag impact point* means the intersection of a predicted ballistic trajectory of an unguided suborbital rocket stage or other impacting component with the Earth's surface. A drag impact point reflects the effects of atmospheric influences as a function of drag forces and mach number.

(2) *Maximum range trajectory* means an optimized trajectory, extended through fuel exhaustion of each stage, to achieve a maximum downrange drag impact point.

(3) *Nominal trajectory* means the trajectory that an unguided suborbital rocket will fly if all rocket aerodynamic parameters are as expected without error, all rocket internal and external systems perform exactly as planned, and there are no external perturbing influences, such as winds, other than atmospheric drag and gravity.

(4) *Normal flight* means all possible trajectories of a properly performing unguided suborbital rocket whose drag impact point location does not deviate from its nominal location more than three sigma in each of the uprange, downrange, left crossrange, or right crossrange directions.

(5) *Performance error parameter* means a quantifiable perturbing force that contributes to the dispersion of a drag impact point in the uprange, downrange, and cross-range directions of an unguided suborbital rocket stage or other impacting launch vehicle component. Performance error parameters for the launch of an unguided suborbital rocket reflect rocket performance variations and any external forces that can cause offsets from the nominal trajectory during normal flight. Performance error parameters include thrust, thrust misalignment, specific impulse, weight, variation in firing times of the stages, fuel flow rates, contributions from the wind weighting safety system employed, and winds.

(c) *Input.* A trajectory analysis requires the inputs necessary to produce a six-degree-of-freedom trajectory. When employing commercially available trajectory software or any trajectory software developed specifically for a launch, a launch operator must identify the following as inputs to the trajectory computations:

(1) *Launcher data.* Geodetic latitude and longitude; height above sea level; location errors; and launch azimuth and elevation.

(2) *Reference ellipsoidal earth model.* Name of the earth model employed, semi-major axis, semi-minor axis, eccentricity, flattening parameter, gravitational parameter, rotation angular velocity, gravitational harmonic constants, and mass of the earth.

(3) *Vehicle characteristics for each stage.* A launch operator shall identify the following for each stage of an unguided suborbital rocket's flight:

(i) Nozzle exit area of each stage.

(ii) Distance from the rocket nose-tip to the nozzle exit for each stage.

(iii) Reference drag area and reference diameter of the rocket including any payload for each stage of flight.

(iv) Thrust as a function of time.

(v) Propellant weight as a function of time.

(vi) Coefficient of drag as a function of mach number.

(vii) Distance from the rocket nose-tip to center of gravity as a function of time.

(viii) Yaw moment of inertia as a function of time.

(ix) Pitch moment of inertia as a function of time.

(x) Pitch damping coefficient as a function of mach number.

(xi) Aerodynamic damping coefficient as a function of mach number.

(xii) Normal force coefficient as a function of mach number.

(xiii) Distance from the rocket nose-tip to center of pressure as a function of mach number.

(xiv) Axial force coefficient as a function of mach number.

(xv) Roll rate as a function of time.

(xvi) Gross mass of each stage.

(xvii) Burnout mass of each stage.

(xviii) Vacuum thrust.

(xix) Vacuum specific impulse.

(xx) Stage dimensions.

(xxi) Weight of each spent stage.

(xxii) Payload mass properties.

(xxiii) Nominal launch elevation and azimuth.

(4) *Launch events.* Stage ignition times, stage burn times, and stage separation times, referenced to ignition time of first stage.

(5) *Atmosphere.* Density as a function of altitude, pressure as a function of altitude, speed of sound as a function of altitude, temperature as a function of altitude.

(6) *Wind errors.* Error in measurement of wind direction as a function of altitude and wind magnitude as a function of altitude, wind forecast error, such as error due to time delay from wind measurement to launch.

(d) *Methodology for determining the nominal trajectory and nominal drag impact points.* A launch operator shall employ steps (d)(1)–(d)(3) of this section to determine the nominal trajectory and the nominal drag impact point locations for each impacting rocket stage and component:

(1) A launch operator shall identify each performance error parameter associated with the unguided suborbital rocket's design and operation and the value for each parameter that reflect nominal rocket performance. These performance error parameters include thrust misalignment, thrust variation, weight variation, fin misalignment, impulse variation, aerodynamic drag variation, staging timing variation, stage separation-force variation, drag error, uncompensated wind, launcher elevation angle error, launcher azimuth angle error, launcher tip-off, and launcher location error.

(2) A launch operator shall perform a no-wind trajectory simulation using a six-degrees-of-freedom (6–DOF) trajectory simulation with all performance error

parameters set to their nominal values to determine the impact point of each stage or component. The 6–DOF trajectory simulation must provide rocket position translation along three axes of an orthogonal earth centered coordinate system and rocket orientation in roll, pitch and yaw. The 6-DOF trajectory simulation must compute the translations and orientations in response to forces and moments internal and external to the rocket including the effects of the input data required in paragraph (c) of this section. The FAA will permit a launch operator to incorporate the following assumptions in a 6–DOF trajectory simulation:

(i) The airframe may be treated as a rigid body.

(ii) The airframe may have a plane of symmetry coinciding with the vertical plane of reference.

(iii) The vehicle may assume to have aerodynamic symmetry in roll.

(iv) The airframe may have six degrees-of-freedom.

(v) The aerodynamic forces and moments may be functions of mach number and may be linear with small flow incidence angles of attack.

(3) A launch operator shall tabulate the geodetic latitude and longitude of the launch vehicle's nominal drag impact point as a function of trajectory time and the final nominal drag impact point of each planned impacting stage or component.

(e) *Methodology for determining maximum downrange drag impact points.* A launch operator shall compute the maximum possible downrange drag impact point for each rocket stage and impacting component. A launch operator shall use the nominal drag impact point methodology defined in paragraph (d) of this section modified to optimize the unguided suborbital rocket's performance and flight profile to create the conditions for a maximum downrange drag impact point, including fuel exhaustion for each stage and impacting component.

(f) *Methodology for computing drag impact point dispersions.* A launch operator shall employ the steps in paragraphs (f)(1)–(f)(3) of this section when determining the dispersions in terms of drag impact point distance standard deviations in uprange, downrange, and crossrange direction from the nominal drag impact point location for each stage and impacting component:

(1) For each stage of flight, a launch operator shall identify the plus and minus one-sigma values for each performance error parameter identified in accordance with paragraph (d)(1) of this section (i.e., nominal value plus one standard deviation and nominal value minus one standard deviation). A launch operator shall determine the dispersion in downrange, uprange, and left and right crossrange for each impacting stage and component. This is done by either performing a Monte Carlo analysis that assumes a normal distribution of each performance error parameter or by determining the dispersion by a root-sum-square method in accordance with paragraph (f)(2) of this section.

(2) When using a root-sum-square method to determine dispersion, a launch operator shall determine the deviations for a given stage by evaluating the deviations produced in that stage due to the performance errors in that stage and all preceding stages of the launch vehicle as illustrated in Table C417–1, and by computing the square root of the sum of the squares of each deviation caused by each performance error parameter's one sigma dispersion for each stage in each of the right crossrange, left crossrange, uprange and downrange directions. A launch operator shall evaluate the performance errors for one stage at a time, with the performance of all subsequent stages assumed to be nominal. A launch operator's root-sum-square method must incorporate the following requirements:

TABLE C417–1.—ILLUSTRATIVE SIMULATION RUNS REQUIRED TO DETERMINE DRAG IMPACT POINT DISPERSIONS FOR A THREE STAGE LAUNCH VEHICLE.

Trajectory simulation runs stage performance error parameters	Dispersion being determined		
	Stage 1	Stage 2	Stage 3
Stage 1 errors	X [1]		
Stage 1 errors, Stage 2 nominal	X		
Stage 1 nominal, Stage 2 errors	X		
Stage 1 errors, Stage 2 nominal, Stage 3 nominal	X		
Stage 1 nominal, Stage 2 errors, Stage 3 nominal	X		
Stage 1 nominal, Stage 2 nominal, Stage 3 errors	X		

[1] An X in a given stage column indicates that the noted simulation runs are required to determine the dispersion for that stage.

(i) With the 6–DOF trajectory simulation used to determine nominal drag impact points in accordance with paragraph (d) of this section, perform a series of trajectory simulation runs for each stage and planned ejected debris such as a fairing, payload, or other component, and, for each simulation, model only one performance error parameter set to either its plus or minus one-sigma value. All other performance error parameters for a given simulation run must be set to their nominal values. Continue until a trajectory simulation run is performed for each plus one-sigma performance error parameter value and each minus one-sigma performance error parameter value for the stage or the planned ejected debris being evaluated. For each trajectory simulation run and for each impact being evaluated, tabulate the downrange, uprange, left crossrange, and right crossrange drag impact point distance deviations measured from the nominal drag impact point location for that stage or planned debris.

(ii) For uprange, downrange, right crossrange, and left crossrange, compute the square root of the sum of the squares of the distance deviations in each direction. The square root of the sum of the squares distance value for each direction represents the one-sigma drag impact point dispersion in that direction. For a multiple stage rocket, perform the first stage series of simulation runs with all subsequent stage performance error parameters set to their nominal value. Tabulate the uprange, downrange, right crossrange, and left crossrange distance deviations from the nominal impact for each subsequent drag impact point location caused by the first stage one-sigma performance error parameter. Use these deviations in determining the total drag impact point dispersions for the subsequent stage impacts as described in paragraph (f)(2)(iii) of this section.

(iii) For each subsequent stage impact of an unguided suborbital rocket, determine the one-sigma impact dispersions by first determining the one-sigma distance deviations for that stage impact caused by each preceding stage as described in paragraph (f)(2)(ii) of this section. Then perform a series of simulation runs and tabulate the uprange, downrange, right crossrange, and left crossrange drag impact point distance deviations as described in paragraph (f)(2)(i) for that stage's one-sigma performance error parameter values with the preceding stage performance parameters set to nominal values. For each uprange, downrange, right crossrange, and left crossrange direction, compute the square root of the sum of the squares of the second stage impact distance deviations due to that stage's and each preceding stage's one-sigma performance error parameter values. This square root of the sum of the squares distance value for each direction represents the total one-sigma drag impact point dispersion in that direction for the nominal drag impact point location of that stage. Use these deviations when determining the total drag impact point dispersions for the subsequent stage impacts.

(3) A launch operator shall determine a three-sigma dispersion area for each impacting stage or component as an ellipse that is centered at the nominal drag impact point location and has semi-major and semi-minor axes along the uprange, downrange, left crossrange, and right crossrange axes. The length of each axis must be three times as large as the total one-sigma drag impact point dispersions in each direction.

(g) *Trajectory analysis products for a suborbital rocket.* A launch operator shall submit the following products of a trajectory analysis for an unguided suborbital rocket to the FAA in accordance with § 417.235(g):

(1) A description of the process that the launch operator used for performing the trajectory analysis including the number of simulation runs and the process for any Monte Carlo analysis performed.

(2) A description of all assumptions and procedures the launch operator used in deriving each of the performance error parameters and their standard deviations.

(3) Launch point origin data: name, geodetic latitude (+N), longitude (+E), geodetic height, and launch azimuth measured clockwise from true north.

(4) Name of reference ellipsoid earth model used. If a launch operator employs a reference ellipsoid earth model other than WGS–84, Department of Defense World Geodetic System, Military Standard 2401 (Jan. 11, 1994), a launch operator shall identify the semi-major axis, semi-minor axis, eccentricity, flattening parameter, gravitational parameter, rotation angular velocity, gravitational harmonic constants (e.g., J2, J3, J4), and mass of earth.

(5) If a launch operator converts latitude and longitude coordinates between different ellipsoidal earth models to complete a trajectory analysis, the launch operator shall submit the equations for geodetic datum conversions and a sample calculation for converting the geodetic latitude and longitude coordinates between the models employed.

(6) A launch operator shall submit tabular data that lists each performance error parameter used in the trajectory computations and each performance error parameter's plus and minus one-sigma values. If the launch operator employs a Monte Carlo analysis method for determining the dispersions about the nominal drag impact point, the tabular data must list the total one-sigma drag impact point distance deviations in each direction for each impacting stage and component. If the launch operator employs the square root of the sum of the squares method described in paragraph (f)(2) of this section, the tabular data must include the one-sigma drag impact point distance deviations in each direction due to each one-sigma performance error parameter value for each impacting stage and component.

(7) A launch operator shall submit a graphical depiction showing geographical landmasses and the nominal and maximum range trajectories from liftoff until impact of the final stage. The graphical depiction must plot trajectory points in time intervals of no greater than one second during thrusting flight and for times corresponding to ignition, thrust termination or burnout, and separation of each stage or impacting body. If there are less than four seconds between stage separation or other jettison events, a launch operator must reduce the time intervals between plotted trajectory points to 0.2 seconds or less. The graphical depiction must show total launch vehicle velocity as a function of time, present-position ground-range as a function of time, altitude above the reference ellipsoid as a function of time, and the static stability margin as a function of time.

(8) A launch operator shall submit tabular data that describes the nominal and maximum range trajectories from liftoff until impact of the final stage. The tabular data must include the time after liftoff, altitude above the reference ellipsoid, present position ground range, and total launch vehicle velocity for ignition, burnout, separation, booster apogee, and booster impact of each stage or impacting body. The launch operator shall submit the tabular data for the same time intervals required by paragraph (g)(7) of this section.

(9) A launch operator shall submit a graphical depiction showing geographical landmasses and the unguided suborbital rocket's drag impact point for the nominal trajectory, the maximum impact range boundary, and the three-sigma drag impact point dispersion area for each impacting stage or component. The graphical depiction must show the following in relationship to each other: the nominal trajectory, a circle whose radius represents the range to the farthest downrange impact point that results from the maximum range trajectory, and the three-sigma drag impact point dispersions for each impacting stage and component.

(10) A launch operator shall submit tabular data that describes the nominal trajectory, the maximum impact range boundary, and each three-sigma drag impact point dispersion area. The tabular data must include the geodetic latitude (positive north of the equator) and longitude (positive east of the Greenwich Meridian) of each point describing the nominal drag impact point positions, the maximum range circle, and each three-sigma impact dispersion area boundary. Each three-sigma dispersion area shall be described by no less than 20 coordinate pairs. All coordinates must be rounded to the fourth decimal point.

C417.5 Hazard Area Analysis

(a) *General.* A launch operator shall perform a hazard area analysis for the flight of an unguided suborbital rocket as required by § 417.235(c). A launch operator shall establish hazard areas to protect the public from planned events during the flight of an unguided suborbital rocket. A launch operator's hazard area analysis must determine a flight hazard area around the launch point and impact hazard areas, aircraft hazard areas, and ship hazard areas for each impacting stage and component in accordance with this section. Requirements for a launch operator's implementation of a hazard area are contained in § 417.121(e) and § 417.121(f) of part 417.

(b) *Hazard area analysis input.* A launch operator shall employ the following inputs to determine each hazard area for the flight of an unguided suborbital rocket:

(1) The launch vehicle downrange, uprange, and crossrange impact dispersion determined in accordance with C417.3 of this appendix.

(2) Latitude and longitude of the nominal impact point of each impacting stage and impacting component determined in accordance with C417.3 of this appendix.

(3) Total propellant weight and propellant type for each rocket stage.

(c) *Methodology for computing a flight hazard area.* A launch operator shall determine a flight hazard area for the flight of an unguided suborbital rocket in accordance with the following:

(1) On the surface of the Earth, a flight hazard area must encompass the blast area surrounding the launch point. A launch operator shall calculate a blast hazard area for an overpressure of 3.0 pounds per square inch that is defined by a circle with the launch point at its center and with a radius R determined using the following equation:

$$R = 20.3\ (NEW)^{1/3}$$

Where:

R is in feet.

NEW = Net explosive weight = W×C

W is the propellant weight in pounds.

C is the TNT equivalency coefficient of the propellant being evaluated. A launch operator shall identify the TNT equivalency of each propellant on its launch vehicle, including any payload. TNT equivalency data for common liquid propellants is provided in tables C417–2. Table C417–3 provides factors for converting gallons of specified liquid propellants to pounds.

(2) In addition to the area on the surface of the Earth determined according to paragraph (c)(1) of this section, for the protection of aircraft, a launch operator's flight hazard area must include an air space region that encompasses the unguided suborbital rocket's three-sigma trajectory dispersion from the Earth's surface at the launch point to an altitude of 60,000 feet.

(d) *Maximum impact range area.* A launch operator shall define a maximum impact range area as a circle with a radius equal to the range of the furthest maximum downrange impact point determined according to C417.3(e).

(e) *Impact hazard areas.* A launch operator shall determine an impact hazard area for each impacting stage and component as depicted in Figure C417–1.

(f) *Planned impact aircraft hazard area.* A launch operator shall employ the methodology described in this paragraph to determine an aircraft hazard area for each planned impact of a launch vehicle stage or component for all suborbital and orbital launches. A launch operator shall compute an aircraft hazard area for each planned impact of a launch vehicle stage or component in accordance with the following:

(1) An aircraft hazard area must be a three dimensional air space region from the Earth's surface to an altitude of 60,000 feet that encompasses, for all altitudes, the larger of the three-sigma drag impact ellipse determined in accordance with C417.3(f)(3) or the ellipse with the same semi-major and semi-minor axis ratio as the impact dispersion, where, if an aircraft were located on the boundary of the ellipse, the probability of hitting the aircraft would be less than or equal to 1×10^{-8} determined in accordance with paragraph (f)(2) of this section. An example aircraft hazard area is illustrated in Figure C417–2. For the launch of an unguided suborbital rocket, if the impact of a stage or component has a three-

sigma dispersion that results in an aircraft hazard area that is prohibitively too large to implement with air traffic control (ATC), a launch operator may employ an alternate aircraft hazard area. A launch operator shall provide a clear and convincing demonstration, through the licensing process, that any alternate aircraft hazard area provides an equivalent level of safety to the requirements of this section based on analysis of the proposed launch and potential air traffic in the impact hazard area.

(2) A launch operator shall determine an aircraft hazard area ellipse where, if an aircraft were located on the boundary of the ellipse, the probability of hitting the aircraft would be less than or equal to 1×10^{-8}. A launch operator shall use the dimensions of the largest aircraft in the vicinity or, if unknown, the dimensions of a Boeing 747 aircraft. A launch operator shall compute an aircraft hazard area to demonstrate the probability of impact in accordance with the following:

(i) Employ the actual speed of the largest aircraft in the vicinity, or assume the aircraft is traveling at mach 0.8 velocity.

(ii) Determine the distance the aircraft travels during the time that the stage or ejected debris falls through a distance equal to twice the length of the debris plus the depth of the aircraft. The aircraft speed, assuming mach 0.8 if unknown, and the time it takes the debris to fall through the depth of the aircraft determine the distance of travel. A launch operator shall use the following equations to make this determination:

$$\beta = \frac{W}{C_d A}$$

$$V_Z = \sqrt{\frac{2g\beta}{\rho}}$$

$$T_a = \left(H_a + 2\cdot L_R\right) / V_Z$$

$$D_x = V_a \cdot T_a$$

Where:

β is the ballistic coefficient of the stage or ejected debris in pounds per square foot.
W is the weight of the stage or ejected debris in pounds.
A is the area of the stage or ejected debris.
C_d is the coefficient of drag (dimensionless) of the stage or ejected debris.
V_Z is the velocity of the stage or ejected debris in the altitude axis.
g is the gravity constant.
ρ is the density of the atmosphere at the assumed aircraft height in pounds per cubic foot.
T_a is the time that the debris falls through a distance equal to twice the length of the stage or ejected debris plus the depth of the aircraft.
H_a is the depth of the aircraft.
L_R is the length of the stage or ejected debris.
V_a is the aircraft's velocity or 0.8 mach if aircraft velocity is unknown.
D_x is the distance traveled during time T_a.

(iii) The distance of the aircraft from the nominal impact point shall be varied with a constant number of sigma increase in both downrange and crossrange until a probability of impact of $\leq 1\times10^{-8}$ is obtained. This shall be accomplished using the following:

$$A_{SA} = D_X \cdot L_a$$

Where:

A_{SA} is the area traveled by the aircraft during T_a
L_a is the distance from wing tip to wing tip of the aircraft.

Start at σ_c = and iterate the following until P_A is less than 1×10^{-8}:

$$\sigma_c = \sigma_c + 0.1$$

$$y = \sigma_y \cdot \sigma_c$$

$$P_A = \frac{A_{SA}}{2\pi\sigma_x\sigma_y} \cdot \left(\exp - \frac{1}{2}\left(\frac{y}{\sigma^2{}_y}\right)^2\right)$$

Repeat the iteration until PA is less than 1×10^{-8}.

Where:

σ_x is the one sigma distance of debris impact in the downrange direction. σ_y is the one sigma distance of debris impact in the crossrange direction.
y is the crossrange distances from the nominal impact point to the assumed position of the aircraft.
P_A is the aircraft impact probability.

(iv) Once P_A is less than 1×10^{-8}, the aircraft hazard area shall be defined by the following elliptical semi axes:

$$xaxis = \frac{\sigma_x}{\sigma_y} \cdot \sigma_c$$

$$yaxis = \sigma_c$$

(3) A launch operator shall determine the time period during which an aircraft hazard area must be in effect. The launch operator shall ensure that an aircraft hazard area remains in effect from before liftoff until after the launch vehicle stage or component impact has occurred. The time that the hazard area is in effect, through completion of launch, must be greater than the impact time of the smallest hazardous debris piece.

(g) *Collective ship-hit probability analysis for planned impacts.* A launch operator shall use statistical ship density data to determine the collective ship-hit probability for each planned impacting stage or component, in accordance with the requirements of this paragraph, to determine whether the launch operator must survey the impact area for ships and to determine flight commit criteria. If a launch operator demonstrates that the collective ship-hit probability for an impacting stage or component is less than or equal to 1×10^{-5}, a launch operator shall define a ship hazard area, in accordance with paragraph (h) of this section, for which the launch operator need not perform flight day surveillance. If the launch operator fails to demonstrate that the collective ship-hit probability for an impacting stage or component is less than 1×10^{-5}, the launch operator shall perform either a flight day ship-hit probability computation using actual ship location data obtained through surveillance or define the ship-hit ellipses according to paragraph (i) of this section, which the launch operator shall survey on the day of flight. A launch operator's analysis for determining collective ship-hit probability using statistical ship density data must satisfy the following requirements:

(1) A launch operator's analysis must account for the ship density in the three-sigma impact dispersion ellipse surrounding each planned stage or component drag impact point location determined in accordance with C417.3(f)(3). The launch operator shall establish ship density based on the most recent statistical data from maritime reports, satellite analysis, or U.S. government information. The ship density must account for time of day and any other factors that might affect the ship density. The statistical ship density for the impact dispersion ellipse must be multiplied by a safety factor of 10 for use in the collective ship-hit probability analysis unless the launch operator demonstrates the accuracy of its ship density data, clearly and convincingly through the licensing process, and accounts for the associated ship density error in the collective ship-hit probability analysis.

(2) A collective ship-hit probability analysis must use the ship density determined in accordance with paragraph (g)(1) of this section to compute the collective ship-hit probability that exists within the three-sigma impact dispersion ellipse surrounding the nominal drag impact point. The analysis shall be performed by computing the collective ship-hit probability for a series of points located one nautical mile apart within the three-sigma impact dispersion ellipse. A launch operator may assume symmetry in all four quadrants of the three-sigma impact dispersion ellipse. Therefore, the series of points evaluated need only cover the area within one quadrant of the ellipse. A launch operator shall assume that the number of ships at each grid point is equal to the ship density established as the number of ships per square nautical mile. A launch operator shall employ the following procedure and steps to compute the collective ship-hit probability (P_S):

(i) Set x = 0.5 (nautical miles) and y = 0.5 (nautical miles).

(ii) Compute P_A and P_S using the following equations:

$$P_A = N_S \frac{A_{SA}}{2\pi\sigma_x\sigma_y} \cdot \left(\exp - \frac{1}{2}\left(\left(\frac{x}{\sigma_x}\right)^2 + \left(\frac{y}{\sigma_y}\right)^2 \right) \right)$$

$$P_S = \sum 4 \cdot P_A$$

Where:

P_A is the ship-hit probability for each ship location evaluated.

P_S is the collective ship-hit probability and is a running sum total of P_A for all the ship locations evaluated.

The multiplication factor ''4'' in the equation for P_S accounts for the four quadrants of the ellipse.

N_S is the number of ships per square mile.

σ_x is the one-sigma distance of the debris impact dispersion in the downrange direction in nautical miles.

σ_y is the one-sigma distance of the debris impact dispersion in the crossrange direction in nautical miles.

x and y are the downrange and crossrange distances, respectively, from the nominal impact point to the assumed position of the ship in nautical miles.

A_{sa} is the area of the N_S ships in square nautical miles. A launch operator shall assume a ship size of 120,000 square feet, unless the launch operator provides a clear and convincing demonstration that a smaller ship size is the greatest ship size in the vicinity of the planned impact.

(iii) If the current value of y is equal to or less than the crossrange distance to the three-sigma impact dispersion ellipse for the current downrange value of x, increase y by 1 nautical mile and repeat step (ii).

(iv) If the current value of y is greater than the crossrange distance to the three-sigma impact dispersion ellipse for the current downrange value of x, reset y to 0.5 nautical miles.

(v) If the current value of x is equal to or less than the downrange distance to the three-sigma impact dispersion ellipse for the crossrange value of 0.5 nautical miles, increment x by 1 nautical mile and repeat steps (ii) through (iv).

(vi) If the current value of x is greater than the downrange distance to the three-sigma impact dispersion ellipse for the crossrange value of 0.5 nautical miles, the computation of P_S for the planned impact is complete.

(h) *Ship hazard areas, surveillance not required.* If the analysis required by paragraph (g) of this section demonstrates, using statistical ship density data, that the collective ship-hit probability is less than 1×10^{-5} for a planned impacting rocket stage or component, ship surveillance is not required for that impact. The ship hazard area must consist of an area centered on the drag impact point and defined by a three-sigma impact dispersion ellipse or the ship-hit ellipse for one ship determined according to paragraph (i)(2) of this section, whichever ellipse is larger. A launch operator shall ensure that a notice for each ship hazard area is disseminated according to § 417.121(e).

(i) *Ship hazard areas, surveillance required.* If a launch operator is unable to demonstrate, using statistical ship density data, that the collective ship-hit probability for a planned impacting rocket stage or component is less than 1×10^{-5} in accordance with paragraph (g) of this section, a launch operator shall either compute the flight day ship-hit probability of hitting any ship surveyed in the vicinity of the planned impact location according to paragraph (i)(1) of this section or the launch operator shall determine and implement ship-hit ellipses according to paragraph (i)(2) of this section.

(1) *Flight day ship-hit probability computation.* When computing ship-hit probability on the day of flight, a launch operator shall compute of the probability of hitting any ship surveyed in the vicinity of a planned impact location. A launch operator's ship-hit computation must account for the locations of all ships within a five-sigma dispersion on the day of flight within 30 minutes of flight. The analysis must account for the changes in impact locations resulting from the launch day wind weighting operations, the speed of each ship in the vicinity of the impact area, and the ships' predicted location at the time of liftoff. The analysis must demonstrate that the collective probability of hitting a ship during flight is less than 1×10^{-5}. The analysis shall use the following equations to compute the collective ship hit probability for all ships located within a five-sigma dispersion of the impact point.

$$P_A = \frac{A_{SA}}{2\pi\sigma_x\sigma_y} \cdot \left(\exp - \frac{1}{2}\left(\left(\frac{x}{\sigma_x}\right)^2 + \left(\frac{y}{\sigma_y}\right)^2 \right) \right)$$

$$P_S = \sum P_A$$

Where:

P_S is the collective ship-hit risk.

P_A is the individual ship-hit risk.

σ_x is the one sigma distance of debris impact dispersion in the downrange direction.

σ_y is the one sigma distance of debris impact dispersion in the crossrange direction.

x and y are the downrange and crossrange distances from the nominal impact point to the assumed position of the ship.

A_{sa} is the area of the ship. A launch operator shall assume a ship size of 120,000 square feet unless the launch operator provides a clear and convincing demonstration that a smaller ship size is the greatest ship size in the vicinity of the planned impact.

(2) *Ship-hit ellipses.* When implementing ship-hit ellipses for a planned impacting rocket stage or component, a launch operator shall compute ship-hit ellipses in accordance with the following:

(i) For each planned impact, a launch operator shall compute ship-hit ellipses for one to 10 ships in increments of one ship. For a given number of ships, the associated ship-hit ellipse must encompass an area around the nominal drag impact point where if the ships were located on the boundary of the ellipse, the probability of impacting one of the ships would be less than or equal to 1×10^{-5}.

(ii) A ship-hit ellipse must have the same semi-major and semi-minor axis ratio as the dispersion of the impacting rocket stage or component.

(iii) When computing a ship-hit ellipse, a launch operator shall assume a ship size of 120,000 square feet unless the launch operator provides a clear and convincing demonstration that a smaller ship size is the greatest ship size in the vicinity of the planned impact.

(iv) For a given number of ships, the distance of each ship from the nominal impact point shall be varied with a constant number of sigma increase in crossrange until a hit probability of $\leq 1\times10^{-5}$ obtained. This shall be accomplished by:

Starting at ($\sigma_C = 0$ and iterating the following until P_S is less than 1×10^{-5}:

$$\sigma_c = \sigma_c + 0.1$$

$$y = \sigma_y \cdot \sigma_c$$

$$P_S = N_S \frac{A_S}{2\pi\sigma_x\sigma_y} \exp\left(-\frac{1}{2}\left(\frac{y}{\sigma_y}\right)^2 \right)$$

Repeat the iteration until P_S is less than 1×10^{-5}.

Where:

σ_y is the one sigma distance of debris impact dispersion in the crossrange direction.

y is the crossrange distance from the nominal impact point to the assumed position of the ship.

(v) Once P_S is less than 1×10^5, the ship hazard contour is defined by the following elliptical semi axis:

$$xaxis = \frac{\sigma_x}{\sigma_y} \cdot \sigma_c$$

$$yaxis = \sigma_c$$

(3) *Implementation of ship-hit methods.* The launch operator's operational methods for implementing either the ship-hit ellipse method or the flight day ship-hit probability computation method must account for the changing impact points resulting from launch day wind weighting operations. Although the last vehicle stage wind impact point is targeted for the nominal impact point, the impact points for each intermediate stage and planned ejected debris will change due to winds. The launch operator shall develop operational methods flight commit criteria to account for the changing impact locations.

(4) *Notice of ship hazard areas.* When employing the ship-hit ellipse method or the flight day ship-hit probability computation method a launch operator shall ensure that a notice of ship hazard areas is disseminated according to § 417.121(e). For the purpose of the notices, a launch operator shall use an area centered on the drag impact point and defined by a three-sigma impact dispersion ellipse or the ship-hit ellipse for one ship determined according to paragraph (i)(2) of this section, whichever ellipse is larger.

(j) *Hazard area analysis products.* A launch operator shall submit the following products of a hazard area analysis for an unguided suborbital rocket to the FAA in accordance with § 417.235(c):

(1) A description of the methodology used to determine each hazard area.

(2) For each hazard area, each source of input data, and a sample of each calculation used to determine the hazard area.

(3) A graphic depiction of each hazard area displaying the centroid of ellipses and lengths of semi-major and semi-minor axes. The graphical depiction of the maximum impact range area and impact hazard area must also include geographical features of the surrounding area.

(4) A description of the methods used to survey for ships and the safety reporting and evaluation of the ship-hit risk.

(5) A description and justification for the source of the ship density data, a description of the method used to compute the collective risk for the three-sigma area about each nominal drag impact point, and the results of the collective ship-hit risk analysis.

C417.7 Wind Weighting Analysis

(a) *General.* As part of a wind weighting safety system, a launch operator shall perform a wind weighting analysis to determine launcher azimuth and elevation settings that correct for the windcocking and wind-drift effects on an unguided suborbital rocket due to forecasted winds in the airspace region of flight. A launch operator's wind weighting safety system and its operation must be in accordance with § 417.125(c). The launch azimuth and elevation settings resulting from a launch operator's wind weighting analysis must produce a trajectory, under actual wind conditions, that results in a final stage drag impact point that is the same as the final stage's nominal drag impact point determined according to C417.3(d).

(b) *Wind weighting analysis constraints.* A launch operator's wind weighting analysis must incorporate the following constraints:

(1) A wind weighting analysis must account for the winds in the airspace region through which the rocket will fly. A launch operator's wind weighting safety system must include an operational method of determining the winds at all altitudes that the rocket will reach up to the maximum altitude defined by dispersion analysis in accordance with C417.3.

(2) A wind weighting analysis must account for an estimation of the uncorrected wind errors that result from the analytical and operational methods employed, including the error resulting from the time between wind measurements.

(3) A wind weighting analysis must account for the dispersion of all impacting debris, including any uncorrected wind error accounted for in the trajectory analysis performed in accordance with C417.3.

(4) A wind weighting analysis must establish flight commit criteria that are a function of the analysis and operational methods employed and reflect the maximum wind velocities and wind variability for which the results of the wind weighting analysis are valid.

(5) A wind weighting analysis must account for the wind effects during each thrusting phase of an unguided suborbital rocket's flight and each ballistic phase of each rocket stage and component until burnout of the last stage.

(6) A wind weighting analysis must account for all errors due to the methods used to measure the winds in the airspace region of the launch, delay associated with wind measurement, and the method used to model the effects of winds. The resulting sum of these error components must be no greater than those used as the wind error dispersion parameter in the launch vehicle trajectory analysis defined in C417.3.

(7) A launch operator shall determine the impact point location for any parachute recovery of a stage or component. The launch operator's wind weighting analysis shall account for any parachute impact or the launch operator shall perform a wind drift analysis to determine the parachute impact point.

(8) A launch operator shall perform a wind weighting analysis using a six-degrees-of-freedom (6–DOF) trajectory simulation that targets an impact point using an iterative process. The resulting trajectory data must account for the performance error parameters used in the trajectory analysis performed according to C417.3. The 6–DOF simulation must account for launch day wind direction and wind magnitude as a function of altitude.

(9) A launch operator shall perform a wind weighting analysis using a computer program or other method of editing wind data, recording the time the data was obtained, and recording the balloon number or identification of any other measurement device used for each wind altitude layer.

(c) *Methodology for performing a wind weighting analysis.* A launch operator's method for performing a wind weighting analysis on the day of flight must incorporate the following:

(1) A launch operator shall measure the winds on the day of flight to determine wind velocity and direction. A launch operator's process for measuring winds must provide wind data that is consistent with the launch operator's trajectory and drag impact point dispersion analysis and any assumptions made in that analysis regarding the actual wind data available on the day of flight. Wind measurements shall be made at altitude increments that do not exceed 200 feet and that are consistent with the launch operator's drag impact point dispersion analysis. Winds shall be measured from the ground level at the launch point to a maximum altitude that is consistent with the launch operator's drag impact point dispersion analysis. The maximum wind measurement altitude must be the apogee of the flight or 90,000 feet, whichever is lower. A launch operator's wind measuring process must employ the use of balloons and radar tracking or balloons fitted with a Global Positioning System transceiver, and must incorporate the following unless the launch operator demonstrates clearly and convincingly, through the licensing process, that an alternate wind measuring approach provides an equivalent level of safety:

(i) Measure winds for the range of altitudes from ground level to the maximum altitude within six hours before flight and after any weather front passes the launch site before liftoff. Wind measurements shall be continued up to the maximum altitude whenever the wind measurements, for any given altitude, from a subsequent balloon release are not consistent with the wind measurements, for the same altitude, from an earlier higher altitude balloon release.

(ii) Measure winds for the range of altitudes from ground level to an altitude of not less than 50,000 feet within four hours before flight and after any weather front passes the launch site before liftoff. Wind measurements to the 50,000-foot altitude shall be repeated whenever the wind measurements, for any given altitude, from a subsequent lower altitude balloon release are not consistent with the wind measurements, for the same altitude, from the 50,000-foot balloon release.

(iii) Measure winds for the range of altitudes from ground level to an altitude of no less than 5,000 feet twice within 30 minutes of liftoff.

(2) A launch operator shall perform runs of the 6–DOF trajectory simulation using the flight day measured winds as input and targeting for the nominal final stage drag impact point. In an iterative process, vary the launcher elevation angle and azimuth angle settings for each simulation run until the nominal final stage impact point is achieved. The launch operator shall use the resulting launcher elevation angle and azimuth angle settings to correct for the flight day winds. The launch operator shall not initiate flight unless the launcher elevation angle and azimuth angle settings after wind weighting are in accordance with the following:

(i) The launcher elevation angle setting resulting from the wind weighting analysis must not exceed ±5° from the nominal launcher elevation angle setting and must not exceed a total of 86°. A launch operator's nominal launcher elevation angle setting must be in accordance with § 417.125(c)(3).

(ii) The launcher azimuth angle setting resulting from the wind weighting analysis must not exceed ± 30° from the nominal launcher azimuth angle setting unless the launch operator demonstrates clearly and convincingly, through the licensing process, that its unguided suborbital rocket has a low sensitivity to high wind speeds and the launch operator's wind weighting analysis and wind measuring process provide an equivalent level of safety.

(3) Using the trajectory produced in paragraph (c)(2) of this section, for each intermediate stage and planned ejected component, compute the impact point that results from wind drift by performing a run of the 6–DOF trajectory simulation with the launcher angles determined in paragraph (c)(2) of this section and the flight day winds from liftoff until the burnout time or ejection time of the stage or ejected component. The resulting impact point(s) must be accounted for when performing flight day ship-hit operations defined in C417.5(i).

(4) If a parachute is used for any stage or component, a launch operator shall determine the wind drifted impact point of the stage or component using a 6–DOF trajectory simulation that incorporates modeling for the change in aerodynamics at parachute ejection. This simulation run is performed in addition to any simulation of spent stages without parachutes.

(5) A launch operator shall verify that the launcher elevation angle and azimuth angle settings at the time of liftoff are the same as required by the wind weighting analysis.

(6) A launch operator shall monitor and verify that any wind variations and maximum wind limits at the time of liftoff are within the flight commit criteria established according to § 417.113(b).

(7) A launch operator shall generate output data from its wind weighting analysis for each impacting stage or component in printed, plotted, or computer medium format. This data shall be made available to the FAA upon request and must include:

(i) Wind measurement data resulting from each wind weighting balloon.

(ii) The results of each computer run made using the data from each wind weighting balloon, including but not limited to, launcher settings, and impact locations for each stage or component.

(iii) Any anemometer data recorded.

(iv) Final launcher settings recorded.

(d) *Wind weighting analysis products.* The products of a launch operator's wind weighting analysis to be submitted to the FAA in accordance with § 417.235(g) must include the following:

(1) A launch operator shall submit a description of its wind weighting analysis methods, including its method and schedule of determining wind speed and wind direction for each altitude layer.

(2) A launch operator shall submit a description of its wind weighting safety system and identify all equipment used to perform the wind weighting analysis, such as any wind towers, balloons, or Global Positioning System wind measurement system employed and the type of trajectory simulation employed.

(3) A launch operator shall submit a sample wind weighting analysis using actual or statistical winds for the launch area and provide samples of the output required in paragraph (c)(7) of this section.

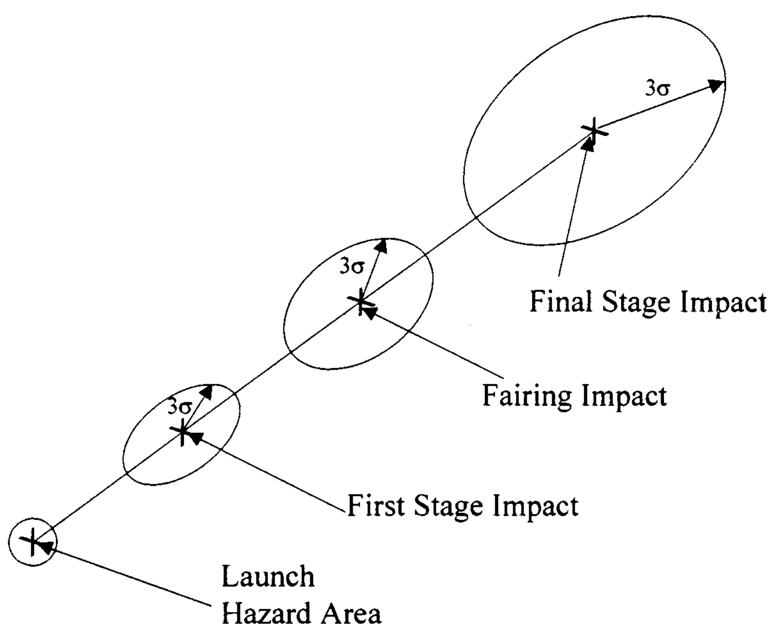
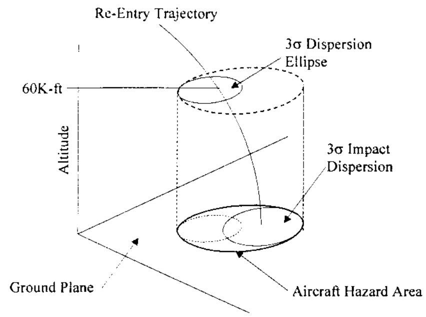


Figure C417-1, Illustration of Planned Impact Hazard Areas



Re-Entry Trajectory Hazard Volume

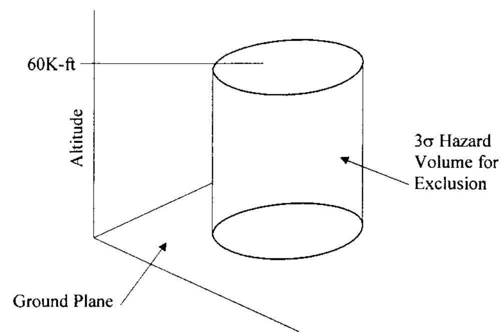


Figure C417-2, Illustration of a Planned Impact Aircraft Hazard Area

TABLE C417–2.—LIQUID PROPELLANT EXPLOSIVE EQUIVALENTS

Propellant Combinations:	
LO_2/LH_2	The larger of $8W^{2/3}$ or 14% of W. Where W is the weight of LO_2/LH_2.
LO_2/LH_2 + LO_2/RP–1	Sum of (20% for LO_2/RP–1) + the larger of: $8W^{2/3}$ or 14% of W. Where W is the weight of LO_2/LH_2.
LO_2/RP–1	20% of W up to 500,000 pounds Plus: 10% of W over 500,000 pounds, Where W is the weight of LO_2/RP–1.
N_2O_4/N_2H_4 (or UDMH or UDMH/N_2H_4 Mixture)	10% of W, Where W is the weight of the propellant.

TABLE C417–3.—PROPELLANT HAZARD AND COMPATIBILITY GROUPINGS AND FACTORS TO BE USED WHEN CONVERTING GALLONS OF PROPELLANT INTO POUNDS

Propellant	Hazard group	Compatibility group	Pounds/gallon	°F
Hydrogen Peroxide	II	A	11.6	68
Hydrazine	III	C	8.4	68
Liquid Hydrogen	III	C	0.59	−423
Liquid Oxygen	II	A	9.5	−297
Nitrogen Tetroxide	I	A	12.1	68
RP–1	I	C	6.8	68
UDMH	III	C	6.6	68
UDHM/Hydrazine	III	C	7.5	68

Appendix D to Part 417—Flight Termination System Components and Circuitry

D417.1 General

(a) This appendix contains requirements that are common to flight termination system components and circuitry and requirements that apply to specific components. A launch operator shall ensure that the flight termination system used in flight satisfies the system level requirements provided in part 417, subpart D and meets the component and circuitry requirements contained in this appendix unless the launch operator demonstrates, clearly and convincingly through the licensing process, that an alternative provides an equivalent level of safety.

(b) The design of each flight termination system component must provide for the component to be tested in accordance with appendix E of this part.

(c) A launch operator shall ensure that compliance with each requirement in this appendix is documented as part of a safety review document prepared during the licensing process according to § 415.107 of this chapter. A licensee shall submit any change to the FAA for approval as a license modification.

D417.3 Design Environments

(a) *General.* The design of each component must provide for the component to accomplish its intended function when subjected to the non-operating and operating environments defined in this section. This section defines the component design environments and the design margins above the maximum predicted environment levels. A launch operator shall establish maximum predicted environment levels according to § 417.307(b) of this part.

(b) *Thermal environment.* The design of a component must provide for the component to function without degradation in performance when exposed to preflight and flight thermal cycle environments. Each thermal cycle, from ambient temperature to one extreme of the required thermal range and then to the other extreme and then back to ambient temperature, must be continuous. The required design thermal range and number of cycles for a component must be in accordance with the following:

(1) *Passive components.* Unless otherwise permitted, the design of a passive component must provide for the component to function without degradation in performance when subjected to eight thermal cycles from one extreme of the maximum predicted thermal range to the other extreme and 24 thermal cycles at temperature extremes of 10 °C lower to 10 °C higher than the maximum predicted thermal range, or from −34 °C to +71 °C, whichever is more severe, with a one hour dwell time at each temperature extreme. The thermal rate of change must be no less than the greater of the maximum predicted thermal rate of change or 1 °C per minute.

(2) *Electronic components.* An electronic flight termination system component is any component that contains active electronic piece parts such as microcircuits, transistors, and diodes. The design of an electronic component must provide for the component to function without degradation in performance when subjected to 18 thermal cycles from one extreme of the maximum predicted thermal range to the other extreme and when subjected to 24 thermal cycles at temperature extremes of 10 °C lower to 10 °C higher than the maximum predicted thermal range, or from −34 °C to +71 °C, whichever is more severe, with a one hour dwell time at each temperature extreme. The thermal rate of change must be no less than the greater of the maximum predicted thermal rate of change or 1 °C per minute.

(3) *Power source thermal design.* The design of a flight termination system power source, including any battery, must provide for the power source to function within its performance specification when exposed to preflight and flight thermal environments. The thermal rate of change must be no less than the greater of the maximum predicted thermal rate of change or 1 °C per minute. The thermal range and number of cycles must be in accordance with the following:

(i) A silver zinc battery must perform within its performance specification when subjected to eight thermal cycles at 10 °C lower to 10 °C higher than its maximum predicted temperature range with a one-hour dwell time at each temperature extreme.

(ii) A nickel cadmium battery must perform within its performance specification when subjected to 24 thermal cycles at 10 °C lower to 10 °C higher than its maximum predicted temperature range or a qualification workmanship screening temperature range of −20 °C to +40 °C, whichever is more severe, with a one-hour dwell time at each temperature extreme.

(iii) All other power sources must perform within their performance specifications when subjected to 24 thermal cycles at 10 °C lower to 10 °C higher than the maximum predicted temperature range with a one-hour dwell time at each temperature extreme.

(4) *Electro-mechanical safe and arm devices with internal explosives.* The design of a safe and arm device must provide for it to function without degradation in performance when subjected to eight thermal cycles from one extreme of the maximum predicted thermal range to the other extreme and when subjected to 24 thermal cycles at temperature extremes of 10 °C lower to 10 °C higher than the maximum predicted thermal range, or from −34 °C to +71 °C, whichever is more severe. The dwell time at each temperature extreme shall last for one hour. The thermal rate of change must be no less than the greater of the maximum predicted thermal rate of change or 1 °C per minute.

(5) *Ordnance thermal design.* The design of an ordnance device and any associated hardware must provide for the ordnance device to withstand eight thermal cycles from extremes of 10 °C lower to 10 °C higher than the maximum predicted thermal range, or from −54 °C to +71 °C, whichever is more severe, with a two hour dwell time at each temperature extreme. Thermal rate of change must be no less than the maximum predicted thermal rate of change or 3 °C per minute whichever is greater.

(c) *Random vibration.* The design of a component must provide for the component to function without degradation in performance when exposed to a composite vibration level profile consisting of the higher of 6 dB above the maximum predicted flight random vibration level or a $12.2G_{rms}$ workmanship screening level, across the 20 Hz to 2000 Hz spectrum of the two levels. The design must provide for the component to function without degradation in performance when exposed to three times the maximum predicted random vibration duration time or three minutes per axis, whichever is greater, on each of three mutually perpendicular axes and where the frequency ranges from 20 Hz to 2000 Hz.

(d) *Sinusoidal vibration.* The design of a component must provide for the component to function without degradation in performance when exposed to 6 dB above the maximum predicted flight sinusoidal vibration level. The design must provide for the component to function without degradation in performance when exposed to three times the maximum predicted sinusoidal vibration duration time on each of three mutually perpendicular axes and where the frequency ranges from 50% lower to 50% greater than the maximum predicted frequency range.

(e) *Transportation vibration.* The design of a component must provide for the component to function without degradation in performance when exposed to 6 dB above the maximum predicted transportation vibration level to be experienced when the component is in the configuration in which it is transported, with an exposure of three times the maximum predicted transportation exposure time. A component must also withstand, without degradation in performance, the workmanship screening vibration levels and duration required by E417.9(f) of appendix E.

(f) *Pyrotechnic shock.* The design of a flight termination system component must provide for the component to function without degradation in performance when exposed to a force of 6 dB above the maximum predicted pyrotechnic shock level to be experienced during flight or a workmanship screening force of 1300 G, whichever is greater. The design must provide for the component to function without degradation in performance after three shocks performed for each of three mutually perpendicular axes, for each direction, positive and negative and where the shock frequency response ranges from 100 Hz to 10,000 Hz.

(g) *Transportation shock.* The design of a flight termination system component must provide for the component to function without degradation in performance after being exposed to the maximum predicted shock to be experienced during transportation while in the configuration in which it is transported.

(h) *Bench handling shock.* The design of a flight termination system component must provide for the component to function without degradation in performance after being exposed to the maximum predicted shock to be experienced during handling in its unpacked configuration.

(i) *Acceleration environment.* The design of a flight termination system component must provide for the component to function without degradation in performance when exposed to launch vehicle breakup acceleration levels of G-forces or twice the maximum predicted flight acceleration levels, whichever is greater. The design must provide for the component to function without degradation in performance when exposed to three times the maximum predicted acceleration duration for each of three mutually perpendicular axes.

(j) *Acoustic environment.* The design of a flight termination system component must provide for the component to function without degradation in performance when exposed to 6 dB above the maximum predicted sound pressure level. The design must provide for the component to function without degradation in performance when exposed to three times the maximum predicted sound pressure duration time or three minutes, whichever is greater for each of three mutually perpendicular axes. The frequency range shall be from 20 Hz to 2000 Hz.

(k) *Other environments.* The design of a flight termination system component must provide for the component to function without degradation in performance after being subjected to temperature, humidity, salt fog, dust, fungus, explosive atmosphere, and electromagnetic energy environments where applicable to flight termination system transportation, storage, pre-flight processing, or preflight system testing and any other environment to which the component could be exposed.

D417.5 Flight Termination System Electrical Components and Electronic Circuitry

(a) *General.* A launch operator's flight termination system must employ electrical components and electronic circuitry that are designed in accordance with this section in addition to meeting the requirements contained in this appendix for specific components.

(b) *Electronic piece parts.* Piece-parts used in electrical components and electronic circuitry must satisfy appendix F of this part.

(c) *Over and under input voltage protection.* A flight termination system component must function reliably and not sustain damage when subjected to the maximum input voltage of the open circuit voltage of its power source and when subjected to the minimum input voltage of the loaded voltage of the power source.

(d) *Series redundant circuit.* A flight termination system component that uses series redundant branches in a firing circuit to satisfy the prohibition against a single failure point must possess monitoring circuits or test points for verifying the integrity of each redundant branch during testing performed after assembly in accordance with appendix E of this part.

(e) *Power control and switching.* In the event of an input power dropout, a power control or switching circuit, including solid-state power transfer switches and arm and enable circuits, must not change state for 50 milliseconds or more. Any electromechanical, solid-state, or relay component used in a flight termination system firing circuit must be capable of delivering the maximum firing current for no less than 10 times the duration of the intended firing pulse.

(f) *Circuit isolation, shielding, and grounding.* The circuitry of a flight termination system component must be shielded, filtered, grounded, or otherwise isolated to preclude any energy sources, internal or external to the launch vehicle, such as electromagnetic energy, static electricity, or stray electrical currents from causing interference that would inhibit the flight termination system from functioning or cause an undesired output of the system. An electrical firing circuit must have a single point ground connection direct to the power source only.

(g) *Circuit protection.* Any circuit protection provided within a flight termination system must be in accordance with the following:

(1) Electronic circuitry must not contain fuses or other similar protection devices. A destruct circuit may employ current limiting resistors.

(2) For any electronic circuit designed to shut down or disable a launch vehicle engine and that interfaces with launch vehicle functions, a launch operator must protect the circuit from over-current including any direct short. This protection must be accomplished through the use of fuses, circuit breakers, or limiting resistors.

(3) The design of a flight termination system output circuit that interfaces with other launch vehicle circuits must prevent any launch vehicle circuit failure from disabling or degrading the flight termination system's performance.

(h) *Repetitive functioning.* All circuitry, elements, components and subsystems of a flight termination system must be capable of withstanding, without degradation in performance, repetitive functioning for five times the expected number of cycles required for acceptance, checkout and operations including re-tests caused by schedule or other delays.

(i) *Watchdog circuits.* Watchdog circuits that automatically shutdown or disable circuitry when specific parameters are violated must not be used in a flight termination system or component except under the provisions of D417.1(a).

(j) *Self-test capability.* If a flight termination system component uses a microprocessor, the component and the microprocessor must be designed to perform self-tests, detect errors, and relay the results through telemetry during flight to the launch operator. The execution of a self-test must not inhibit the intended processing function of the unit or cause any output to change.

(k) *Electromagnetic interference protection.* The design of a flight termination system component must eliminate the possibility of the maximum predicted electromagnetic interference emissions or susceptibilities, whether conducted or radiated, from affecting the component's performance. A launch operator shall ensure that the electromagnetic interference susceptibility level of a component provides for the component to function without degradation in performance when subjected to the maximum predicted emission levels of all other launch vehicle components and external sources to which the component would be exposed.

(l) *Ordnance initiator circuits.* The design of any ordnance initiator circuit that is part of a flight termination system must be in accordance with the following:

(1) An ordnance initiator circuit must deliver an operating current of at least 150% of the initiator's all-fire qualification current level when operating at the lowest battery voltage and under the worse case system tolerances allowed by the system design limits.

(2) For a low voltage ordnance initiator with an electro-explosive device that initiates at less than 50 volts, the initiator's circuitry must limit the power at each associated electro-explosive device that could be produced by an electromagnetic environment to a level at least 20 dB below the pin-to-pin direct current no-fire power of the electro-explosive device.

(3) For a high voltage ordnance initiator that initiates ordnance at greater than 1000 volts, safe and arm plugs must be used to interrupt power to the main initiator's charging circuits, such as the trigger and output capacitors. The design of a high voltage initiator's circuitry must ensure that the power that could be produced at the initiator's command input by an electromagnetic environment is limited to no greater than 20 dB below the initiator's firing level.

D417.7 Flight Termination System Monitor, Checkout, and Control Circuits

(a) All monitor, checkout, and control circuits must take their measurement directly from the parameter being monitored. A launch operator shall ensure that the monitor circuits monitor the parameters required by § 417.321(a).

(b) All monitor, control and checkout circuits must be independent of any firing circuit. A monitor, control, or and checkout circuit must not share a connector with a firing circuit.

(c) No monitor, checkout, or control circuit may be routed through a safe and arm plug.

(d) Any monitor and checkout current in an electro-explosive device system firing line must not exceed one-tenth of the no-fire current of the electro-explosive device.

(e) Resolution, accuracy, and data rates for each monitoring circuit must allow for detecting when specifications are exceeded and detecting out-of-family conditions. A launch operator shall ensure that resolution, accuracy, data rates, and maximum and minimum values are specified for each flight termination system parameter monitored.

D417.9 Flight Termination System Ordnance Train

(a) An ordnance train must consist of all components responsible for initiation, transfer and output of an explosive charge. Ordnance train components must include, but need not be limited to, initiators, energy transfer lines, boosters, explosive manifolds, and destruct charges.

(b) The reliability of an ordnance train to initiate ordnance, including the ability to propagate a charge across any ordnance interface, must be 0.999 at a 95% confidence level.

(c) The decomposition, cook-off, sublimation, auto-ignition, and melting temperatures of all flight termination system ordnance must be at least 30°C higher than the maximum predicted environmental temperature to which the material will be exposed during storage, handling, installation, transportation, and flight.

(d) An ordnance train must include initiation devices that can be connected or removed from the destruct charge as late in the launch countdown as possible. The design of an ordnance train must provide for easy access to the initiation devices.

D417.11 Radio Frequency Receiving System

(a) *General.* A radio frequency receiving system must include each flight termination system antenna and radio frequency coupler and any radio frequency cable or other passive device used to connect a flight termination system antenna to a command receiver. A radio frequency receiving system must deliver command control system radio frequency energy within its performance specification to each flight termination system command receiver when subjected to performance degradation caused by command control system transmitter variations, non-nominal launch vehicle flight conditions, and flight termination system hardware performance variations.

(b) *Sensitivity.* A radio frequency receiving system must provide command signals to each command receiver decoder at an electromagnetic field intensity of 12dB above the level required for reliable receiver operation. The 12dB margin must be met over 95% of the antenna radiation sphere surrounding the launch vehicle when accounting for command control system radio frequency transmitter characteristics and path loses due to atmospheric conditions, plume attenuation, aspect angle, and any other attenuation factor. The 12dB margin must be met at any point along the launch vehicle trajectory where the flight safety system is required to work.

(c) *Testing.* A radio frequency receiving system shall be tested in accordance with E417.17 of appendix E of this part. The design of a radio frequency receiving system must provide for acquisition of the test data that verifies the functional performance of the radio frequency receiving system.

(d) *Antenna.* Each flight termination system antenna must be in accordance with the following:

(1) The design of a flight termination system antenna must provide for a radio frequency bandwidth that exceeds two times the total combined maximum tolerances of all applicable radio frequency performance factors. The performance factors must include frequency modulation deviation of multiple tones, command control transmitter inaccuracies, and variations in hardware performance during thermal and dynamic environments.

(2) Any thermal protection used on a flight termination system antenna is part of the antenna and must be subjected to all the antenna system requirements for design, test, and antenna pattern measurement.

(3) A flight termination system antenna must be compatible with the command control system transmitting equipment.

(e) *Radio frequency coupler.* A launch operator shall use a passive radio frequency coupler to combine radio frequency signals inputs from each flight termination system antenna and distribute the required signal level to each command receiver. The FAA will evaluate the use of any active radio frequency coupler on a case-by-case basis. A radio frequency coupler shall be in accordance with the following:

(1) The design of a radio frequency coupler must provide for the elimination of any single point failure in one redundant command receiver or antenna from affecting any other redundant command receiver or antenna. This shall be accomplished by providing isolation between each port. A launch operator shall ensure that each input port is isolated from all other input ports, each output port is isolated from all other output ports and that all input ports are isolated from all output ports such that an open or short circuit in one redundant command destruct receiver or antenna path will not prevent the functioning of the other command destruct receiver or antenna path.

(2) The design of a radio frequency coupler must provide for a radio frequency bandwidth that exceeds two times the total combined maximum tolerances of all applicable radio frequency performance factors. The performance factors must include frequency modulation deviation of multiple tones, command control transmitter inaccuracies, and variations in hardware performance during thermal and dynamic environments.

D417.13 Electronic Components

(a) *General.* The requirements in this section apply to all command receiver decoders and any other electronic component that contains piece-part circuitry and is part of a flight termination system. Piece-parts used in an electronic component must be in accordance with appendix F of this part.

(b) *Response time.* Each electronic component's response time must be such that the total flight termination system response time, from receipt of a destruct command sequence to initiation of destruct output, is less than or equal to the response time used in the time delay analysis required by § 417.223(b)(3).

(c) *Wire and connectors.* All wire and connectors used in an electronic component must be in accordance with D417.17 of this appendix.

(d) *Adjustment.* An electronic component must not require any adjustment after successful completion of acceptance testing.

(e) *Self-test.* The design of an electronic component that uses a microprocessor must provide for the component to perform a self-test, detect errors, and relay the results through telemetry during flight to the launch operator. The execution of a self-test must not inhibit the intended processing function of the unit or cause any output to change state.

(f) *Electronic component repetitive functioning.* The design of an electronic component including all circuitry and parts must provide for the electronic component to withstand, without degradation in performance, repetitive functioning for five times the total expected number of cycles required for acceptance tests, pre-flight tests, and flight operations, including an allowance for potential retests due to schedule delays.

(g) *Acquisition of test data.* An electronic component shall be tested according to appendix E of this part. The design of an electronic component must allow for separate component testing and the recording of parameters that verify its functional performance, including the status of any command output, during testing.

(h) *Warm-up time.* Each electronic component's warm-up time, that ensures reliable operation, must be less than or equal to the warm-up time that is incorporated into the preflight testing performed for each countdown according to § 417.317(h)(4).

(i) *Electronic component circuit protection.* The design of an electronic component must provide circuit protection for power and control circuitry, including switching circuitry, that ensures the component does not degrade in performance when subjected to launch processing and flight environments. An electronic component's circuit protection must be in accordance with the following:

(1) Circuit protection must provide for an electronic component to function without degradation in performance when subjected to the maximum input voltage of the open circuit voltage of the component's power source and when subjected to the minimum input voltage of the loaded voltage of the power source.

(2) In the event of an input power dropout, any control or switching circuit critical to the reliable operation of a component, including solid-state power transfer switches, must not change state for at least 50 milliseconds.

(3) Watchdog circuits that automatically shutdown or disable an electronic component when specific parameters are violated must not be used except under the provisions of D417.1(a).

(4) The performance of an electronic component must not degrade when any of its monitoring circuits or nondestruct output ports are subjected to a short circuit or the highest positive or negative voltage capable of being supplied by the monitor batteries or other power supplies.

(5) An electronic component must function without degradation in performance when subjected to any undetectable reverse polarity voltage that can occur during launch processing.

(j) *Electromagnetic interference susceptibility.* The design of an electronic component must eliminate the possibility of electromagnetic interference or modulated or unmodulated radio frequency emissions from affecting the component's performance. These electromagnetic interference and radio frequency environments include emissions or susceptibilities, whether conducted or radiated.

(1) A launch operator shall ensure that the susceptibility level of an electronic component is below the emissions of all other launch vehicle components and external transmitters.

(2) Any electromagnetic emissions from an electronic component must not be at a level that would affect the performance of other flight termination system components.

(3) An electronic component must not produce inadvertent command outputs when subjected to potential external radio frequency sources and modulation schemes to which the component could be subjected prior to and during flight.

(k) *Output functions and monitoring.* The design of an electronic component must provide for the following output functions and monitoring:

(1) Each series redundant branch in any firing circuit of an electronic component that prevents a single failure point from issuing a destruct output must include a monitoring circuit or test points that verify the integrity of each redundant branch after assembly.

(2) Any piece-part used in a firing circuit must have the capacity to output at least 1.5 times the maximum firing current for no less than 10 times the duration of the maximum firing pulse.

(3) An electronic component's destruct output circuit and all its parts must have the capacity to deliver output power to the intended output load while operating with

any input voltage that is within the component's input power operational design limits.

(4) An electronic component must include monitoring circuits that provide for monitoring the health and performance of the component including the status of any command output.

(5) The maximum leakage current through an electronic component's destruct output port must not degrade the performance of down-string circuitry or ordnance initiation systems or result in inadvertent initiation of ordnance.

D417.15 Command Receiver Decoder

(a) *General.* A command receiver decoder must function when subjected to performance degradation caused by command control system transmitter variations and non-nominal launch vehicle flight. This shall be accomplished in accordance with the requirements of this section.

(b) *Electronic component.* A command receiver decoder must be in accordance with the requirements for all electronic components provided in D417.13 of this appendix.

(c) *Radio frequency processing.* Radio frequency processing circuitry within a command receiver decoder must provide for the command receiver decoder to function in the flight radio frequency environment in accordance with the following:

(1) A command receiver decoder must function at the command control system transmitter frequency to be used during flight. A command receiver decoder must function according to its performance specifications at twice the worst-case command control system transmitter frequency modulation variations.

(2) The lowest guaranteed radio frequency sensitivity of a command receiver decoder must be in accordance with the 12dB link margin provided by the radio frequency receiving system as required by D417.11(b). A command receiver decoder must not be so sensitive that it would respond to extraneous signals, including external radio frequency sources in the area of the launch point. The design of a command receiver decoder must provide for its sensitivity to be repeatable within ±3dB throughout its lifetime when tested under similar conditions.

(3) A command receiver decoder must function, including processing of arm and destruct signals, when exposed to the maximum radio frequency energy that the command control system transmitter is capable of producing plus a 3 dB margin without change or degradation in performance after such exposure.

(4) A command receiver decoder must function, including processing of arm and destruct signals, at its threshold sensitivity when subjected to twice the worst-case radio frequency shift of the carrier center frequency and command tone modulation that could occur due to factors such as command control system transmitting equipment performance variations, flight doppler shifts, or local oscillator instability.

(5) The design of a command receiver decoder must protect against performance degradation when exposed to an external transmitter of less power than the command control system transmitter. The application of any unmodulated radio frequency at a power level up to 80% of the command control system transmitter's modulated carrier signal must not capture the receiver or interfere with a signal from the command control system.

(6) A command receiver decoder must output a signal strength monitor that is directly related and proportional to the radio frequency input signal. The linear region from threshold to saturation must have a dynamic range of at least 50 dB.

(7) A command receiver decoder must not produce an inadvertent output when subjected to a radio frequency input short-circuit, open-circuit, or any change in input voltage standing wave ratio.

(d) *Decoder logic.* Decoder logic circuitry must provide for a command receiver decoder to function in accordance with the following:

(1) A command receiver's decoder must reliably process a command signal sequence of tones at twice the worst-case tolerances associated with the command control system transmitting equipment.

(2) A command receiver decoder's tone filter must have a bandwidth that ensures accurate recognition of the command signal tone. The receiver decoder must distinguish between tones that are capable of inhibiting or inadvertently issuing an output command.

(3) The arm command must be a prerequisite for the destruct command. Once the arm command is processed, a command receiver decoder must be single fault tolerant against an inadvertent destruct.

(4) The design of a command receiver decoder must provide for the decoding and output of a tone, such as a pilot tone or check tone, that is representative of link and command closure. The presence or absence of this tone signal must have no effect on a command receiver decoder's command processing and output capability.

(5) Tone sequences used for arm and destruct must protect against inadvertent or unintentional destruct actions.

D417.17 Wiring and Connectors

(a) A launch operator shall ensure that the design of each cable, connector, and wire that interfaces with any flight termination system component is qualified as part of the component qualification testing performed according to appendix E of this part.

(b) All wiring and connectors that interface with flight termination system components must have electrical continuity and electrical dropout protection that ensures the flight termination system components function without degradation in performance.

(c) All wiring and connectors must have shielding that ensures the flight termination system's performance will not be degraded or experience an inadvertent destruct output when subjected to electromagnetic interference levels 20 dB greater than the greatest electromagnetic interference induced by launch vehicle and launch site systems.

(d) The dielectric withstanding voltage between mutually insulated portions of any component part must provide for the component to function at the component's rated voltage and withstand momentary over-potentials due to switching, surge, or any other similar event without degradation in performance.

(e) The insulation resistance between mutually insulated portions of any component must provide for the component to function at its rated voltage and the insulation material must not deteriorate due to workmanship, heat, dirt, oxidation or loss of volatile material.

(f) The insulation resistance between wire shields and conductors, and between each connector pin must be capable of withstanding a minimum workmanship voltage of at least 1500 volts, direct current, or 150 percent of the rated output voltage, whichever is greater.

(g) For loads that will be experienced with continuous duty cycles of greater than 100 seconds, all wiring and connector pins must be sized to carry 150% of the design load. For loads that will be experienced for less than 100 seconds, all wiring and insulation must provide a design margin greater than the wire insulation temperature specification.

(h) All cables and connectors must not degrade in performance when subjected to the greatest pull force that could be experienced during manufacturing or installation or due to any unexpected handling environment that could go undetected.

(i) Redundant flight termination system circuits must not share any wiring harness or connector.

(j) For any connector or pin connection that is not functionally tested once connected as part of a flight termination system or component, the design of the connector or pin connection must eliminate the possibility of a bent pin, mismating, or misalignment.

(k) A bent connector pin that makes unintended contact with another pin or the case of the connector or component or results in an open circuit must not result in inadvertent initiation. A flight termination system component must be designed to prevent undetectable damage or overstress from occurring as the result of a bent pin.

(l) In addition to requirements of this section, all connectors must satisfy the piece part requirements of appendix F of this part.

(m) All connectors must positively lock to prevent inadvertent disconnection during launch vehicle processing and flight.

D417.19 Batteries

(a) *Capacity.* A flight termination system battery must have a capacity that is indicated on its name plate and is no less than the sum total amp-hour and pulse capacity needed for load and activation checks, launch countdown checks, any potential hold time, any potential number of preflight re-tests due to potential schedule delays including the launch operator's desired number of potential launch attempts before the battery would have to be replaced, plus a flight capacity allowance. The flight capacity allowance must be no less than 150% of the capacity needed to support a normal flight from liftoff to the no longer endanger time determined in accordance with § 417.221(c) and must allow for two arm and two destruct command loads at the end of the flight. In addition, for a launch vehicle that uses solid propellant, the flight capacity allowance must be greater than or equal to the capacity need to support a 30-minute hang-fire hold time.

(b) *Electrical characteristics.* A flight termination system battery must have the following electrical characteristics:

(1) The lowest allowed battery voltage, including all load conditions, must be the flight termination system electrical components' minimum acceptance-test voltage in accordance with the test requirements of appendix E of this part. For a pulse application used to fire an electro-explosive device, the voltage supplied by a battery under all potential load conditions must be greater than or equal to the lowest qualification test voltage applicable to the associated electrical components according to appendix E of this part.

(2) A battery that provides power to an electro-explosive device initiator must:

(i) Deliver 150% of the electro-explosive device's all-fire current at the qualification test level. The battery must deliver the current to the ordnance initiator at the lowest allowed system battery voltage.

(ii) Have a current pulse duration ten times greater than the duration required to initiate the electro-explosive device or a minimum workmanship screening level of 10 seconds, whichever is greater.

(iii) Have a pulse capacity of no less than twice the expected number of arm and destruct command sets planned during launch vehicle processing, preflight flight termination system end-to-end tests, plus flight commands including load checks, conditioning, and firing of initiators.

(3) The design of a battery and its activation procedures must ensure uniform cell voltage after activation including any battery conditioning needed to ensure uniform cell voltage, such as peroxide removal or nickel cadmium preparation. A launch operator shall ensure that the same activation procedures are used to activate batteries for qualification testing and to activate flight batteries.

(4) The design of a battery must permit open circuit voltage and load testing of each cell when assembled in the battery case during and after activation.

(5) The design of a battery and cell must protect against undetectable damage resulting from reverse polarity, shorting, overcharging, thermal runaway, and overpressure.

(c) *Service and storage life.* The service and storage life of a flight termination system battery must be in accordance with the following:

(1) A flight termination system battery must have a total activated service life that provides for the battery to meet the capacity and electrical characteristics required by paragraphs (a) and (b) of this section.

(2) A flight termination system battery must have a specified storage life. The design of a battery must provide for meeting the activated service life requirement in paragraph (c)(1) of this section after being subjected to its storage life, whether stored in an activated or inactivated state.

(d) *Monitoring capability.* The design of a battery must provide for monitoring the status of battery voltage and current being drawn. Monitoring accuracy must be consistent with the minimum and maximum voltage and current limits to be used for launch countdown. The design of a battery that requires heating or cooling to sustain performance must provide for monitoring the battery's temperature.

(e) *Manufacturing controls.* Each flight termination system battery production lot must be subjected to destructive and nondestructive acceptance testing in accordance with appendix E of this part unless a launch operator demonstrates during the licensing process that all cell and battery parts, materials and manufacturing processes are documented and under configuration control. A launch operator may submit any associated battery documentation and configuration control procedures and processes to the FAA during the licensing process for approval on a case-by-case basis.

(f) *Battery identification.* Each battery must be permanently labeled with the component name, type of construction (including chemistry), manufacturer identification, part number, lot and serial number, date of manufacture, and storage life.

(g) *Battery heaters.* The design of a battery heater must ensure uniform temperature regulation of all battery cells.

(h) *Silver zinc batteries.* A silver zinc battery that is part of a flight termination system must meet the requirements of paragraphs (a) through (g) of this section and the following:

(1) A silver zinc battery must consist of cells with electrode plates, all of which are from the same production lot.

(2) The design of a silver zinc battery must allow activation of individual cells within the battery.

(3) For any silver zinc battery that may leak electrolyte as part of normal operations, the battery's performance must not be degraded when the battery experiences the greatest normal electrolyte migration. Degradation in performance includes changes in pin-to-case or pin-to-pin resistances that are outside the design limits.

(4) The design of a silver zinc battery and its cells must allow for the qualification, acceptance, and storage life extension testing required by appendix E of this part. A launch operator shall ensure sufficient batteries and cells are available to accomplish the required testing.

(5) For each battery, one additional cell with the same lot date code shall be attached to the battery for use in cell acceptance verification tests. The cell shall be attached to the battery from the time of assembly until performance of the acceptance tests to ensure that the additional cell is subjected to all the same environments as the complete battery.

(i) *Rechargeable batteries, such as nickel cadmium batteries.* A rechargeable battery, such as a nickel cadmium battery, that is part of a flight termination system must meet the requirements in paragraphs (a) through (g) of this section and the following:

(1) Each charge and discharge cycle of a rechargeable flight termination system battery must provide the capacity and electrical characteristics required by paragraphs (a) and (b) of this section.

(2) A rechargeable battery must meet its performance specifications for five times the number of operating charge and discharge cycles expected of the battery throughout its life, including all acceptance testing, preflight testing, and flight.

(3) Each rechargeable battery and each of the battery's cells must consistently retain its charge and provide the capacity margin according to its performance specifications and satisfy the capacity requirements contained in paragraph (a) of this section.

(4) A rechargeable battery must consist of cells from the same production lot.

(5) The design of a nickel cadmium battery and each of its cells must allow for the qualification and acceptance tests required according to appendix E of this part. A launch operator shall ensure sufficient batteries and cells are available to accomplish the required testing. During the licensing process, the FAA may identify and impose additional design and test requirements for any other type of rechargeable battery proposed for use as part of a flight safety system.

D417.21 Electro Mechanical Safe and Arm Devices With an Internal Electro-Explosive Device

(a) A safe and arm device in the arm position must remain in the arm position without degradation in performance when subjected to the design environmental levels determined according to D417.3 of this appendix.

(b) All wiring and connectors used on a safe and arm device must satisfy D417.17 of this appendix.

(c) All piece parts in the firing circuit of a safe and arm device must satisfy appendix F of this part.

(d) A safe and arm device's internal electro-explosive device must satisfy the requirements for an ordnance initiator contained in D417.27 of this appendix.

(e) A safe and arm device must not require any adjustment throughout its service life.

(f) Once armed and locked, a safe and arm device, including all internal ordnance components, must function with a reliability of 0.999 at a 95% confidence level.

(g) A safe and arm device's internal electrical firing circuitry, such as wiring, connectors, and switch deck contacts, must be capable of withstanding, without degradation in performance, an electrical current pulse with an energy level of no less than 150% of the internal electro-explosive device's all-fire energy level for 10 times the all-fire pulse duration. A safe and arm device must be capable of delivering this firing pulse to the internal electro-explosive device without any dropouts when subjected to the design environmental levels.

(h) The design of a safe and arm device must provide for the device to function without degradation in performance after being exposed to any inadvertent transportation, handling, or installation environment that could go undetected.

(i) The design of a safe and arm device must provide for the device to not initiate and be safe to handle after being subjected to the worst-case drop and resulting impact that it could experience during storage, transportation, or installation.

(j) When a safe and arm device's electro-explosive device is initiated, the safe and arm device's body must not fragment, regardless of whether the explosive transfer system is connected or not.

(k) When dual electro-explosive devices are used within a single safe and arm device, the design must ensure that one electro-explosive device does not affect the performance of the other electro-explosive device.

(l) A safe and arm device must not degrade in performance when subjected to five times the total expected number of safe and arm cycles required for acceptance tests, preflight tests, and flight operations, including an allowance for potential re-tests due to schedule changes.

(m) A launch operator shall ensure that a safe and arm device is tested according to appendix E of this part. The design of a safe and arm device must allow for separate component testing and the recording of parameters that verify its functional performance during testing, including the status of any command output.

(n) A safe and arm device must be environmentally sealed to the equivalent of 10^{-4} scc/sec of helium or the device's design must provide other means of withstanding non-operating environments, such as salt-fog and humidity experienced during storage, transportation and preflight testing.

(o) While in the safe position, a safe and arm device must prevent degradation in performance or inadvertent initiation of an electro-explosive device during transportation, storage, preflight testing, and preflight failure conditions and must be in accordance with the following:

(1) While in the safe position, a safe and arm device's electrical input firing circuit must prevent degradation in performance or inadvertent initiation of the electro-explosive device when subjected to any continuous external energy source such as static discharge, radio frequency energy, or firing voltage.

(2) While in the safe position, a safe and arm device must prevent the initiation of its internal electro-explosive device and any other ordnance train component, with a reliability of 0.999 at a 95% confidence level.

(3) The performance of a safe and arm device must not degrade when locked in the safe position and subjected to a continuous operational arming voltage with an exposure time of five minutes or the maximum time that could occur operationally, whichever is greater.

(4) A safe and arm device must not initiate its electro-explosive device or any other ordnance train component when locked in the safe position and subjected to a continuous operational arming voltage with an exposure time of be one hour or the maximum time that could occur operationally, whichever is greater.

(5) The design of a safe and arm device must provide for manual and remote status indication when in the safe position. When transitioning from the arm to safe position, the safe indication must not appear unless the position of the safe and arm device has progressed more than 50% beyond the no-fire transition motion.

(6) The design of a safe and arm device must provide for its rotor or barrier to be remotely moved to the safe position from any rotor or barrier position.

(7) The design of a safe and arm device must provide for the device to be manually moved to the safe position.

(8) A safe and arm device must include a safing interlock that prevents movement from the safe position to the arm position while operational arming current is being applied. The design of the interlock must provide for it to be positively locked into place and allow for verification of proper functioning. The interlock removal design or procedure must eliminate the possibility of accidental disconnection of the interlock.

(p) The arming of a safe and arm device must be in accordance with the following:

(1) A safe and arm device is armed when all ordnance interfaces, such as electro-explosive device, rotor charge, and explosive transfer system components are aligned with one another to ensure propagation of the explosive charge.

(2) When in the arm position, the greatest energy supplied to a safe and arm device's electro-explosive device from electronic circuit leakage and radio frequency energy must be no greater than 20 dB below the guaranteed no-fire level of the electro-explosive device.

(3) The design of a safe and arm device must provide a local and remote status indication when the device is in the arm position. The arm indication must not appear unless the safe and arm device has been moved to the locked arm position.

(4) The design of a safe and arm device must provide for the device to be remotely armed.

D417.23 Exploding Bridgewire Firing Unit

(a) *General.* The design of an exploding bridgewire firing unit must be in accordance with the requirements for electronic components contained in D417.13 of this appendix.

(b) *Charging and discharging.* The design of an exploding bridgewire firing unit must provide for the unit to be remotely charged and discharged and allow for an external means to positively interrupt the firing capacitor charging voltage.

(c) *Input command processing.* An exploding bridgewire firing unit's electrical input processing circuitry must be in accordance with the following:

(1) An exploding bridgewire firing unit's input circuitry must function when subjected to the greatest potential electromagnetic interference noise environments without inadvertent triggering.

(2) All series redundant branches in the firing circuit of an exploding bridgewire firing unit that prevent any single failure point from issuing a destruct output must include monitoring circuits or test points for verifying the integrity of each redundant branch after assembly.

(3) The unit input trigger circuitry of an exploding bridgewire firing unit must maintain a minimum 20 dB margin between the threshold trigger level and the worst-case noise environment.

(4) The design of an exploding bridgewire firing unit must provide for a minimum trigger sensitivity of 6 dB higher in amplitude and one-half the time duration of the worst-case trigger signal that could be delivered during flight.

(5) In the event of a power dropout, any control or switching circuit critical to the reliable operation of an exploding bridgewire firing unit, including solid-state power transfer switches must not change state for 50 milliseconds or more.

(6) An exploding bridgewire firing unit's response time must satisfy D417.13(b). An exploding bridgewire firing unit's response time must satisfy its performance specification for the range of input trigger signals from the specified minimum trigger signal amplitude and duration to the specified maximum trigger signal amplitude and duration.

(d) *High voltage output.* An exploding bridgewire firing unit's high voltage discharge circuit must be in accordance with the following:

(1) An exploding bridgewire firing unit must include circuits for capacitor charging, bleeding, charge interruption, and triggering.

(2) The design of an exploding bridgewire firing unit must provide for a single fault tolerant capacitor discharge capability.

(3) The design of an exploding bridgewire firing unit must provide for the unit to deliver a voltage to the exploding bridgewire that is no less than 50% greater than the exploding bridgewire's minimum all-fire voltage, not including transmission losses, at the unit's specified worst-case high and low arming voltages.

(4) The design of an exploding bridgewire firing unit must prevent corona and arcing on internal and external high voltage circuitry.

(5) An exploding bridgewire firing unit must meet its performance specifications at the worst case high and low arm voltages that could be delivered during flight.

(6) Any high energy trigger circuit used to initiate exploding bridgewire firing unit's main firing capacitor must deliver an output signal of no less than a 50% voltage margin above the nominal voltage threshold level.

(e) *Output monitors.* The monitoring circuits of an exploding bridgewire firing unit must provide the data for real-time checkout and determination of the firing unit's acceptability for flight. The monitored data must include the voltage level of all high voltage capacitors and the arming power to the firing unit.

D417.25 Ordnance Interrupter Safe and Arm Device Without an Electro-Explosive Device

(a) Once locked in the arm position, an ordnance interrupter must function to accept a donor explosive transfer system charge and transfer the output detonation to an explosive transfer system acceptor charge's ordnance initiation train with a reliability of 0.999 at a 95% confidence level.

(b) An ordnance interrupter must remain in the arming position and function without degradation in performance when subjected to the design environmental levels determined according to D417.3 of this appendix.

(c) An ordnance interrupter must not require adjustment throughout its service life.